



**State of New York
Andrew M. Cuomo Governor
Competitive Procurement for:**

Public Safety Credentialing and Training System "PSCTS" RFP CJS 2014-01

CONTRACTING ENTITY	DCJS SOLE DESIGNATED CONTACT FOR INQUIRIES AND SUBMISSIONS
State of New York acting by and through the Division of Criminal Justice Services (DCJS) Michael C. Green, Commissioner, On behalf of: Offices, departments, and agencies of the State of New York, certain political subdivisions and authorized users of the DCJS Public Safety Credentialing and Training System	Ms. Kimberly Szady Director, Financial Administration New York State Division of Criminal Justice Services Alfred E. Smith Building 80 South Swan Street, 10th Floor Albany, New York 12210 All questions regarding this RFP must be submitted via electronic mail to the designated contact for this RFP DCJSProcurement@dcjs.ny.gov Neither phone nor fax inquires will be accepted

Calendar of Events	
Event	Date
1. RFP Release Date	August 29, 2014
2. Deadline for Submission of Vendors' Questions	September 10, 2014
3. Issuance of DCJS Response to Submitted Questions	September 17, 2014
4. BID PROPOSALS DUE DATE	September 26, 2014, 4 p.m.
5. Anticipated Notification of Award	October 28, 2014
6. Debriefing Request Deadline	November 3, 2014
7. Bid Protest Deadline	See Protest Procedure at Appendix H
8. Timeframe for Contract Approval	December 29, 2014
9. Timeframe for Replacement of the Public Safety Credentialing and Training System – See Project Schedule in Subsection 3.1.E.2	September 1, 2015

NYS reserves the right, in its sole discretion, to alter the information and schedule shown above. In such an event, NYS will e-mail notice to vendors who have submitted a Bid and publish the notification on its website at:
<http://www.criminaljustice.ny.gov/pio/vendor/business.html>

ALL PROPOSALS SUBMITTED IN RESPONSE TO THIS RFP AND ALL QUESTIONS, COMMUNICATIONS AND SUBMISSIONS TO DCJS MUST BE WRITTEN IN THE ENGLISH LANGUAGE WITH QUANTITIES EXPRESSED USING ARABIC NUMERALS. ALL PRICES SHALL BE EXPRESSED, AND ALL PAYMENTS SHALL BE MADE, IN UNITED STATES DOLLARS (\$ USD). ANY PROPOSAL RECEIVED THAT DOES NOT MEET THE ABOVE CRITERIA MAY BE REJECTED AT THE SOLE OPTION OF DCJS.

NOTICE OF POLICY AND PROHIBITIONS ON PROCUREMENT LOBBYING AND CONTACTS

State Finance Law §139-j(6) requires that a governmental entity incorporate a summary of its policy and prohibitions regarding permissible contacts during a covered procurement. Pursuant to State Finance Law §§139-j and 139-k, this Request for Proposal (RFP) includes and imposes certain restrictions on communications between the Division of Criminal Justice Services (DCJS), a governmental entity and a vendor during the procurement process.

A vendor is restricted from making contacts from the earliest notice of intent to solicit offers including this Request for Proposal through final award and approval of the procurement contract by DCJS and the Office of the State Comptroller (“Restricted Period”) to other than the DCJS staff member who has been designated by DCJS as the sole procurement contact and who has been identified on the cover page of this RFP. There are certain statutory exceptions set forth in State Finance Law §139-j(3)(a).

State Finance Law §139-k(4) obligates every governmental entity during the restricted period of a procurement contract to make a written record of any contacts made. The term “contact” is defined by statute and refers to those oral, written or electronic communications that a reasonable person would infer are attempts to influence the governmental procurement. DCJS is required to make a determination of the responsibility of the vendor pursuant to State Finance Law §§139-j and 139-k. Certain findings of non-responsibility can result in rejection for contract award and in the event of two findings within a four (4) year period; the vendor is debarred from obtaining governmental procurement contracts.

Additional information and guidance on the “Restricted Period” and permissible contacts can be found in the guidelines issued by the New York State Advisory Council on Procurement Lobbying, which can be found on the OGS website at:

<http://www.ogs.ny.gov/ACPL/>

Vendors must provide DCJS with a required affirmation of understanding and agreement to comply with procedures on procurement lobbying restrictions regarding contacts in the restricted period for a procurement contract in accordance with State Finance Law §§139-j and 139-k. The vendor must agree to the certification and complete the affirmation of such

agreement included at Attachment 14 in Form 1: Offerer's Affirmation of Understanding of an Agreement Pursuant to State Finance Law §139-j(3) and §139-j(6)(b) and Form 3: Offerer's Certification of Compliance with State Finance Law §139-k(5), which are a mandatory submissions.

Sole Designated Procurement Contact

All Vendors are required to comply with Chapter 1 of the Laws of 2005, the Procurement Lobbying Act, as amended by Chapter 4 of the Laws of 2010. All questions regarding this RFP must be submitted via electronic mail to the DCJS Sole Designated Contact for this procurement specified on the cover page of this RFP. Pursuant to the Procurement Lobbying Law the DCJS Sole Designated Contact for this procurement specified on the cover page of this RFP is designated as the DCJS Solicitation Contact for this procurement. All inquiries, questions, filings and submission of proposals that are submitted to any other individual or physical address shall not be considered as official, binding, or as having been received by the State. Pursuant to the Procurement Lobbying Law the DCJS Sole Designated Contact for this procurement specified on the cover page of this RFP is designated as the Designated Agency Contact for this procurement. During the Restricted Period for this RFP, all communications shall be directed to the DCJS Sole Designated Contact for this procurement.

DCJS may at its sole option change the sole designated contact and will make notification of such a change by electronic mail to vendors who have filed a Bid and through its website. The webpage Uniform Resource Locator (URL) is provided on the cover pages of this RFP.

Prior Non-responsibility Determination Affirmation

New York State Finance Law §139-k(2) obligates a governmental entity to obtain specific information regarding all prior non-responsibility determinations with respect to State Finance Law §139-j. This information must be collected in addition to the information that is separately obtained pursuant to State Finance Law §163(9). In accordance with State Finance Law §139-k, an Offerer must be asked to disclose whether there has been a finding of non-responsibility made within the previous four (4) years by any governmental entity due to: (a) a violation of State Finance Law §139-j or (b) the intentional provision of false or incomplete information to a governmental entity. The terms “Offerer” and “governmental entity” are defined in State Finance Law § 139-k(1). State Finance Law §139-j sets forth detailed requirements about the restrictions on contacts during the procurement process. A violation of State Finance Law §139-j includes, but is not limited to, an impermissible contact during the restricted period (for example, contacting a person or entity other than the designated contact person, when such Contact does not fall within one of the exemptions).

The Offerer must agree to the certification and complete the affirmation of such agreement included at Attachment 14 in Form 2: Offerer’s Disclosure of Prior Non Responsibility Determinations, which is a mandatory submission.

Offerer Certification of Compliance with State Finance Law §139-k(5)

In addition to any other remedy at law or equity, the DCJS reserves the right to terminate any contract in the event it is found that the certification filed by the Contractor in accordance with New York State Finance Law §139-k was intentionally false or intentionally incomplete. Upon such finding, the Governmental Entity may exercise its termination right by providing written notification to the Contractor in accordance with the written notification terms of the contract.

Public Officers Law Sections 73 and 74

The New York State Joint Commission on Public Ethics (JCOPE), is charged with administering and enforcing the State's ethics and lobbying laws as well as the State's anti-nepotism law and laws pertaining to certain political activities and improper influence. It seeks to insure compliance with the ethical standards that public officials and lobbyists must observe in order to ensure public trust and confidence in government. More information is available at the Commission's website at <http://www.jcope.ny.gov>

The Offerer will ensure that all of its personnel involved in the preparation and submission of the Offerer's proposal(s) have read the Public Officers Code of Ethics, Sections 73 and 74 of the Public Officers Law, and that the Offerer has advised its personnel of their obligation not to importune any violations of those sections. For the convenience of the reader certain sections in effect as of the date of release of this RFP are reproduced below. Readers are advised to check official sources.

Public Officers Law § 73(5)

5. No statewide elected official, state officer or employee, individual whose name has been submitted by the governor to the senate for confirmation to become a state officer or employee, member of the legislature or legislative employee shall, directly or indirectly:

(a) solicit, accept or receive any gift having more than a nominal value, whether in the form of money, service, loan, travel, lodging, meals, refreshments, entertainment, discount, forbearance or promise, or in any other form, under circumstances in which it could reasonably be inferred that the gift was intended to influence him, or could reasonably be expected to influence him, in the performance of his official duties or was intended as a reward for any official action on his part. No person shall, directly or indirectly, offer or make any such gift to a statewide elected official, or any state officer or employee, member of the legislature or legislative employee under such circumstances.

(b) solicit, accept or receive any gift, as defined in section one-c of the legislative law, from any person who is prohibited from delivering such gift pursuant to section one-m of the legislative law unless under the circumstances it is not reasonable to infer that the gift was intended to influence him; or

(c) permit the solicitation, acceptance, or receipt of any gift, as defined in section one-c of the legislative law, from any person who is prohibited from delivering such gift pursuant to section one-m of the legislative law to a third party including a charitable organization, on such official's designation or recommendation or on his or her behalf, under circumstances where it is reasonable to infer that the gift was intended to influence him.

Public Officers Law §74:

Sec. 74. Code of ethics. 1. Definition. As used in this section: The term "state agency" shall mean any state department, or division, board, commission, or bureau of any state department or any public benefit corporation or public authority at least one of whose members is appointed by the governor or corporations closely affiliated with specific state agencies as defined by paragraph (d) of subdivision five of section fifty-three-a of the state finance law or their successors.

The term "legislative employee" shall mean any officer or employee of the legislature but it shall not include members of the legislature.

2. Rule with respect to conflicts of interest. No officer or employee of a state agency, member of the legislature or legislative employee should have any interest, financial or otherwise, direct or indirect, or engage in any business or transaction or professional activity or incur any obligation of any nature, which is in substantial conflict with the proper discharge of his duties in the public interest.

3. Standards.

a. No officer or employee of a state agency, member of the legislature or legislative employee should accept other employment which will impair his independence of judgment in the exercise of his official duties.

b. No officer or employee of a state agency, member of the legislature or legislative employee should accept employment or engage in any business or professional activity which will require him to disclose confidential information which he has gained by reason of his official position or authority.

c. No officer or employee of a state agency, member of the legislature or legislative employee should disclose confidential information acquired by him in the course of his official duties nor use such information to further his personal interests.

d. No officer or employee of a state agency, member of the legislature or legislative employee should use or attempt to use his official position to secure unwarranted privileges or exemptions for himself or others, including but not limited to, the misappropriation to himself, herself or to others of the property, services or other resources of the state for private business or other compensated non-governmental purposes.

e. No officer or employee of a state agency, member of the legislature or legislative employee should engage in any transaction as representative or agent of the state with any business entity

in which he has a direct or indirect financial interest that might reasonably tend to conflict with the proper discharge of his official duties.

f. An officer or employee of a state agency, member of the legislature or legislative employee should not by his conduct give reasonable basis for the impression that any person can improperly influence him or unduly enjoy his favor in the performance of his official duties, or that he is affected by the kinship, rank, position or influence of any party or person.

g. An officer or employee of a state agency should abstain from making personal investments in enterprises which he has reason to believe may be directly involved in decisions to be made by him or which will otherwise create substantial conflict between his duty in the public interest and his private interest.

h. An officer or employee of a state agency, member of the legislature or legislative employee should endeavor to pursue a course of conduct which will not raise suspicion among the public that he is likely to be engaged in acts that are in violation of his trust.

i. No officer or employee of a state agency employed on a full-time basis nor any firm or association of which such an officer or employee is a member nor corporation a substantial portion of the stock of which is owned or controlled directly or indirectly by such officer or employee, should sell goods or services to any person, firm, corporation or association which is licensed or whose rates are fixed by the state agency in which such officer or employee serves or is employed.

4. Violations. In addition to any penalty contained in any other provision of law any such officer, member or employee who shall knowingly and intentionally violate any of the provisions of this section may be fined, suspended or removed from office or employment in the manner provided by law. Any such individual who knowingly and intentionally violates the provisions of paragraph b, c, d or i of subdivision three of this section shall be subject to a civil penalty in an amount not to exceed ten thousand dollars and the value of any gift, compensation or benefit received as a result of such violation. Any such individual who knowingly and intentionally violates the provisions of paragraph a, e or g of subdivision three of this section shall be subject to a civil penalty in an amount not to exceed the value of any gift, compensation or benefit

Freedom of Information Law (FOIL) Requests

To request access, pursuant to the Freedom of Information Law (FOIL), to a record maintained by the Division of Criminal Justice Services, you must make your request in writing. Please be as specific as possible in describing the record(s) in which you are interested. Within five business days of the receipt of a written request, we will send a written acknowledgement that we have received the request. Please send your inquiry via mailing provider, FAX or e-mail to:

Records Access Office
NYS Division of Criminal Justice Services
Alfred E. Smith State Office Building
80 South Swan Street
Albany, NY 12210

Updated: 8/28/2014 10:44 AM

FAX: (518) 457-2416

E-mail: foil@dcjs.ny.gov

Questions or comments: foil@dcjs.ny.gov

TABLE OF CONTENTS

1.0	INTRODUCTION.....	1
1.1	Overview of DCJS' Training and Registry Missions	1
1.2	Purpose of this Request for Proposal (RFP)	1
1.3	Current Public Safety Credentialing and Training System Description	5
1.4	The Future System	5
2.0	ADMINISTRATIVE REQUIREMENTS AND INFORMATION	7
2.1	Information to be Communicated in Writing or by E-mail from NYS.....	7
2.2	Submission of Written Questions	7
2.3	Issuance of Official Responses to Vendors' Questions	7
2.4	Delivery of Proposals.....	7
2.5	Proposal Format and Content Requirements	8
	A. Package 1 - Technical Proposal.....	8
	B. Package 2 – Financial/Administrative Proposal.....	9
2.6	Mandatory Requirement - No Exceptions Permitted.....	11
2.7	NYS Reserves the Right to Modify Requirements	11
2.8	Costs Incurred Prior to Contract Approval	11
2.9	Mandatory Requirement - Price Protection	11
2.10	Procurement Record.....	11
2.11	Notification of Award and Opportunity for Debriefing.....	12
2.12	DCJS Contract Award Protest Procedure	12
2.13	State's Reserved Rights	12
2.14	Contract Term	14
2.15	Time is of the Essence	14
2.16	Contract Formation.....	14
2.17	Mandatory Requirement - Standard Clauses for New York State Contracts.....	15
2.18	Mandatory Requirement for Contracts Estimated to be \$1,000,000 or More.....	16
2.19	Encouraging Use of New York State Businesses in Contract Performance	17
2.20	Mandatory Requirement - Discriminatory Jurisdictions.....	17
2.21	Negotiations with the Next Highest Offerer	17
2.22	Prime Contractor.....	18
2.23	Subcontractors	18
2.24	Trade Secret Materials	20
3.0	SPECIFICATIONS FOR EVALUATION	22
3.1	Technical Specifications	22
	A. Executive Summary	22
	B. Offerer Mandatory Qualifying Experience and Customer References.....	24
	C. Mandatory Requirement – Base Requirements for Offerer's Proposed PSCTS Solution.....	26
	D. Optional Requirements-Separately Priced	40
	E. Project Plan	40
3.2	Cost Specifications.....	45
	A. Proposed Fixed Purchase Price – Mandatory Base System	46
	B. Maintenance and Support Price – Mandatory Base System.....	46
	C. Optional Licensing and Professional Services Price List.....	47
	D. Total Proposed Cost for Offerer's Mandatory Base System for Initial 10 Year Contract Period.....	47
	E. Proposed Fixed-Price Milestone Deliverable Payment Schedule	47

F.	Detailed Optional Features Price List.....	48
G.	Optional Services Price List	48
3.3	Administrative Specifications	48
A.	Firm Offer Letter and Conflict of Interest Disclosure	48
B.	Contract Administration Team.....	49
C.	Mandatory Requirement – MacBride Fair Employment Principles	49
D.	Mandatory Requirement – Non-Collusive Bidding Certification	50
E.	Mandatory Requirement - Procurement Lobbying.....	50
F.	Mandatory Requirement - Provisions of NYS Tax Law §5-A.....	51
G.	Mandatory Requirement – NYS Standard Vendor Responsibility Questionnaire	52
H.	Encouraging Use of NYS Businesses in Contract Performance	52
I.	Proposed Subcontractors	53
J.	Key Subcontractor Certification.....	53
K.	Consultant Disclosure.....	53
L.	Non-Disclosure Agreement.....	54
M.	Staffing Plan	54
N.	MWBE Utilization Plan.....	55
4.0	EVALUATION AND SCORING METHOD	56
4.1	Overall Proposal Evaluation Process	56
4.2	Timeliness and Completeness Review.....	56
4.3	Mandatory Qualifying Experience - Technical Evaluation (Pass / Fail)	57
4.4	Preferred Technical Evaluation (70 Points).....	58
4.5	Financial (Cost) Evaluation (30 Points).....	58
4.6	Final Proposal Ranking.....	59
5.0	OTHER TERMS AND CONDITIONS	60
5.1	Governing Law	60
5.2	Substantial / Material Change.....	60
5.3	Changes in Contractor’s Project Team	61
5.4	Third Party Beneficiary Requirement.....	61
5.5	Qualified Project Personnel	61
5.6	Quality of Service	61
5.7	Ongoing Reports/Documentation	62
5.8	Insurance and Maintenance Bond.....	63
A.	General	63
B.	Payment of Premium & Deductible	63
C.	Carrier(s)	63
D.	Coverage Term.....	64
E.	Form of Insurance	64
F.	Subcontractor Insurance	64
G.	Right to Make Claim	65
H.	Commercial General Liability & Umbrella Liability Insurance	65
I.	Comprehensive Professional Liability Insurance.....	65
J.	Liability Insurance Policies / State Designation.....	66
K.	New York State Worker’s Compensation Law	66
L.	Maintenance Bond.....	68
5.9	Title & Legal Interests	68
A.	Documentation	68
B.	Incorporation into Subcontracts	69
5.10	Submission of Contractor Invoices.....	69

5.11	Payment for Services of Contractor	69
5.12	Warranties	70
	A. Public Safety Credentialing and Training System Performance	70
	B. Conformance to Manufacturer's Specifications	71
	C. Product & Equipment Warranty	71
	D. Title & Ownership Warranty	72
	E. Contractor Compliance	72
	F. Virus Warranty	73
	G. Workmanship Warranty	73
	H. Adequate Parts Supply	73
	I. Data Processing Warranty	73
	J. Personnel Eligible for Employment	74
	K. Survival of Warranties	74
5.13	Indemnification & Limitation of Liability	74
5.14	Software, Customizations, Upgrades	76
	A. Software License	76
	B. Archival Back-up for Licensed Software	76
	C. Transfers or Assignments to a Third Party Agent	76
	D. Confidentiality	77
5.15	Escrow for Software Source Code	77
	A. Escrow	77
	B. Terms of Escrow	77
	C. Changes in Escrow	79
5.16	Compliance with Miscellaneous Laws	79
5.17	Termination	81
	A. For Convenience	84
	B. For Cause	84
	C. Termination Notice	86
	D. Termination Date	87
	E. Mitigation of Costs	87
	F. Asset Accounting & Transfer	87
5.18	Post Termination Transition	88
	A. Post Termination Transition Period	88
	B. No Interruption in Service	88
	C. Post Termination Transition Plan	88
	D. Contractor Post Termination Transition Services	89
	E. Compensation for Post Termination Transition Services	89
	F. State Responsibilities for Post Termination Transition	89
	G. Training Successor Organization & Personnel	89
5.19	Rescale of Project	90
5.20	Process for Change Orders	90
5.21	Force Majeure	90
5.22	Press Releases	91
5.23	Security, Information Security, Breach and Notification Act	91
	A. Security Procedures & Employee Dishonesty	91
	B. Information Security Breach and Notification Act	92
5.24	Indemnification of New York State and Authorized Users for Breach of Security	92
5.25	Nondisclosure & Confidentiality	93
5.26	Security	95
5.27	Criminal Justice Information Services (CJIS)	96
5.28	NYS Cyber Security Policy P03-002	97

5.29	User Data is the Property of DCJS.....	98
5.30	Accounting/Audit.....	99
	A. Maintenance of Supporting Documentation.....	99
	B. Access to & Audit of Agreement Records	99
5.31	Minority & Women Owned Business Enterprises	99
5.32	Payment of Outstanding Tax Liabilities	102
5.33	Integration, Merger & Order of Precedence	102
5.34	Dispute Resolution and Escalation	103
5.35	Additional Responsibilities of the Prime Contractor	104
5.36	New York State Responsibilities	106
5.37	Extension of Existing Product Line – New Products.....	106
5.38	Partial Invalidity	106
5.39	Not Employees of the State.....	107
5.40	Waiver.....	107
5.41	Taxes.....	107
5.42	Extraneous Terms	107
5.43	Severability	108
5.44	Assignment of Claim	108
5.45	Notification	109
5.46	Notice to State.....	109
5.47	Suspension of Work.....	110
5.48	General Provision as to Remedies	110
5.49	Liquidated Damages	110
5.50	Extension of Use	111
5.51	Foreign Nationals.....	112
5.52	Headings Have No Legal Significance	112
5.53	Penalties for Non Performance	112

APPENDIX A -- Standard Clauses for New York State Contracts

APPENDIX B -- General Specifications

APPENDIX C -- MWBE Reports

APPENDIX D -- Criminal Justice Information Services (CJIS) Security Policy

APPENDIX E -- State Consultant Disclosure

APPENDIX F -- Qualifying Customer Reference Questionnaire

APPENDIX G -- Public Safety Credentialing and Training System Informational Tables

APPENDIX H -- DCJS Contract Award Protest Procedure

APPENDIX I -- Key Process Flow Charts

APPENDIX J -- Change Request Form

APPENDIX K -- DCJS Business Requirements

APPENDIX L -- Conversion Plan Requirements

APPENDIX M -- Acceptance Testing Requirements

APPENDIX N -- NYS DCJS Technology Policy, June 4, 2007

APPENDIX O -- Enterprise Information Security Policy v4.0

APPENDIX P -- NYS ITS Portfolio of Supported Platforms

APPENDIX Q -- Web Based Forms Supporting DCJS Business Requirements

APPENDIX R -- Deliverables Acceptance Form

APPENDIX S -- Training Requirements

APPENDIX T -- Glossary of Acronyms

ATTACHMENT 1 -- Questions Template

ATTACHMENT 2 -- Non-Disclosure Agreement

ATTACHMENT 3 -- Not Used Intentionally Blank

ATTACHMENT 4 -- Not Used Intentionally Blank

ATTACHMENT 5 -- Offerer Firm Information Form

ATTACHMENT 6 -- Mandatory Qualifying Experience Customer Reference Form

ATTACHMENT 7 -- PSCTS Mandatory Base System Requirements - COTS or Customized

ATTACHMENT 7a - PSCTS Optional Features – COTS or Customized

ATTACHMENT 8 -- PSCTS Mandatory Base System Requirements - Solutionand/or
Documentation Descriptions with Forms Required for Offerer Bid Response

ATTACHMENT 9 -- Staffing Plan

ATTACHMENT 10 -- MWBE Utilization Plan

ATTACHMENT 11 -- Firm Offer Letter and Conflict of Interest Disclosure

ATTACHMENT 12 -- Non-Discrimination in Employment in Northern Ireland Statement

ATTACHMENT 13 -- Non-Collusive Bidding Certification

ATTACHMENT 14 -- Division of Criminal Justice Services Summary of Policy and Prohibitions
on Procurement Lobbying

- Form 1 – Offerer’s Affirmation of Understanding of and Agreement Pursuant to State Finance Law § 139-j(3) and § 139-j (6) (b)
- Form 2 – Offerer Disclosure of Prior Non-Responsibility Determinations
- Form 3 – Offerer’s Certification of Compliance with State Finance Law § 139-k(5)

ATTACHMENT 15 --Tax Law - Contractor, Affiliate and Subcontractor Sales and Compensation
Use Tax Certification

- N.Y.S. Department of Taxation and Finance Contractor Certification Form ST-220-TD
- N.Y.S. Department of Taxation and Finance Contractor Certification to Covered Agency Form St-220-CA

ATTACHMENT 16 -- Vendor Responsibility Questionnaire

ATTACHMENT 17 -- Encouraging Use of NYS Businesses in Contract Performance

ATTACHMENT 18 -- Proposed Subcontractors

ATTACHMENT 19 -- Key Subcontractor Certification

ATTACHMENT 20 -- Draft Contract with Mandatory Terms and Conditions

ATTACHMENT 21 -- State Consultant Services Contractor’s Annual Employment Report
Addendum

ATTACHMENT 22 -- FBI CJIS Security Addendum

ATTACHMENT 23 -- Proposed Fixed Purchase Price - Mandatory Base System

ATTACHMENT 24 – Maintenance and Support Price - Mandatory Base System

ATTACHMENT 25 – Optional Professional Services Price List

ATTACHMENT 26 – Total Proposed Cost for Offerer's Mandatory Base system for Initial 10 Year Contract Period

ATTACHMENT 27 – Proposed Fixed-Price Milestone Deliverable Payment Schedule

ATTACHMENT 28 – Detailed Optional Features Price List

ATTACHMENT 29 – Optional Services Price List

This Page Intentionally Blank

1.0 Introduction

1.1 Purpose of this Request for Proposal (RFP)

On behalf of New York State the Division of Criminal Justice Services (“DCJS”) is seeking to procure a web based Public Safety Credentialing and Training System (“PSCTS”). This system would be hosted by New York State.

The purpose of this RFP is to purchase software and implementation services for use by New York State Agencies and their respective constituents. The first project to be undertaken under this RFP is to replace the existing DCJS Police and Peace Officer Registry System hereinafter referred to as the PSCTS. The software purchase includes all licensing fees, annual maintenance (patches and support), customization services as required to meet business needs, initial training for DCJS administrative staff and Information Technology support staff, and a comprehensive product manual for DCJS Instructors use in developing training for its customers.

This project is a collaborative effort between DCJS and the NYS Office of Information Technology Services (ITS). ITS will provide the infrastructure and system support services.

Future functionality may be added over time, at New York State’s discretion.

1.2 Overview of DCJS’ Training and Registry Missions

DCJS is a multi-function criminal justice support agency with a variety of statutory responsibilities, ranging from the collection and analysis of statewide crime data; the operation of the DNA databank and criminal fingerprint files; the administration of federal and state criminal justice funds; the support of criminal justice-related agencies across the state; and the administration of the state’s Sex Offender Registry.

Among DCJS’ core agency functions is the oversight of public safety training programs. This portion of the agency’s mission is administered by the DCJS Office of Public Safety (OPS). The mission of OPS is to reduce crime and increase the effectiveness and efficiency of law enforcement, public safety and security organizations located within NYS, and to increase public confidence by promoting professionalism through standardized training and support. OPS is responsible for the administration of both mandated police and peace officer training programs as well as in-service initiatives developed to enhance the productivity and professionalism of public and private law enforcement and public safety personnel as well as security personnel in New York.

Classifications of Law Enforcement Officers in New York State

In New York State, there are two classifications of law enforcement officers; police officers and peace officers. The term *police officer* refers to law enforcement officers whose primary obligation is to prevent, detect, and enforce the general laws of New York State. This group embodies the widely accepted definition of a “police officer” and is

authorized to exercise the greatest amount of law enforcement authority. Criminal Procedure Law (CPL)§1.20(34) identifies 22 titles as police officers.

The term *peace officer* refers to an additional classification of law enforcement officer with more specialized or unique responsibilities confined to a specific locale or type of criminal activity. The primary mission of certain peace officers may not be law enforcement in nature; however, during the performance of those duties, a *peace officer* may occasionally necessitate law enforcement authority to enforce a general, special or local law; charter; rule; judgment or order. For example, correction officers are peace officers with the primary function of care, custody and transport of inmates. Occasionally, a correction officer may necessitate the exercise of law enforcement powers, such as the use of force or the conduct of a warrantless search, when performing their primary duties. CPL§2.10 identifies individual categories of peace officers; and CPL§ 2.16prescribes specific peace officer powers upon other individual employees. The total number of peace officer designations is 134.

There is a third tier of public safety personnel in New York State, security guards. Security guards are civilians employed by a security guard company to protect individuals and property from harm, theft or other unlawful activity; deter, observe, and report incidents in order to prevent any unlawful or unauthorized activity. Security guards are not authorized to exercise any law enforcement powers.

DCJS Oversight of Police Officer and Peace Officer Training Programs

The Municipal Police Training Council (MPTC) is an advisory body within DCJS charged with establishing basic training standards for police officers. Today, the MPTC is a standards setting and monitoring body responsible for determining the minimally acceptable training and employment standards for both police and peace officers in New York State. It recommends rules and regulations for promulgation by the Governor with respect to the administration of police officer, peace officer, campus security officer, and correction officer training programs¹. Once implemented, these rules and regulations have the force and effect of law.

OPS serves as the staff arm to the MPTC and is comprised of two sections, the Administrative Services Unit and the Law Enforcement Training Unit. The Administrative Services Unit is responsible for the regulatory compliance function as specified in State law².

The Administrative Services Unit

In its capacity as staff arm to the MPTC, OPS oversees on behalf of DCJS, the certification of police officers, peace officers, and correction officers who have satisfactorily completed mandated basic training programs and issue certificates to such

¹ Executive Law §§ 839- 840.

² Executive Law §841.

officers; reviews and approves advanced in-service training programs for police officers, peace officers, and correction officers and issues appropriate certificates; and manages the certification of instructors for police, peace and correction officer training programs³. Additionally, the Administrative Services Unit is charged with maintaining DCJS' Central State Registry of Police Officers and Peace Officers.

The primary concern of the Administrative Services Unit is to ensure all training providers maintain compliance with standards established by the MPTC or by DCJS itself. OPS personnel are responsible for the review of basic training and other curricula submitted by law enforcement agencies and training academies as well as for performing both announced and unannounced site visits to verify compliance. This mechanism ensures police training programs conducted throughout the state are uniform and meet the minimum specifications with respect to content, instructors and training hours. In 2013, staff reviewed and certified 1,350 training courses and processed 40,358 student records.

Delivery of Training Programs to Law Enforcement

The Law Enforcement Training Unit

The Law Enforcement Training Unit (LETU) is charged with the development and dissemination of training and information designed to increase the professionalism of public safety organizations through standardized training and support for mandated training programs and curricula. The LETU also provides support for in-service programs such as: human trafficking; clandestine labs; motor vehicle collision investigation; and aides the MPTC in developing model policies for topics such as recording custodial interviews. In 2013, LETU staff delivered training to 10,073 students through 142 in-residence courses and 8 on-line courses.

On-line Training Programs for Law Enforcement

The NYS Department of Health (DOH) is charged with administering the Breath Analysis Operator (BAO) certification program. DCJS is the training agency for the purposes of providing training to law enforcement personnel in the procedures for collecting breath [alcohol] samples⁴. Under BAO program rules, operators are required to recertify every two years.

In 2006, DCJS partnered with a vendor to provide an on-line recertification program for its Breath Analysis Operators. Operators complete the recertification on-line and the data is manually downloaded by OPS staff for entry into the DCJS database. Over 90% of operators now recertify on-line. In 2013, 1,894 Breath Analysis Operators recertified using the on-line application.

As this technology has become more pervasive, the Law Enforcement Training Unit has developed a library of Sharable Content Object Reference Model (SCORM) compliant

³ Executive §§841 and 841-c, Criminal Procedure Law § 2.30, and Education Law §§ 355(l) and 6435(3)

⁴ Title 10 of the *Official Compilation of Codes, Rules and Regulations of the State of New York*, Part 59.

on-line training programs accessible to officers over the internet. These training programs are self-paced and cover cutting-edge topics and technologies available to law enforcement as well as model policy and legal updates.

The Central State Registry of Police Officers and Peace Officers

The Central State Registry of Police Officers and Peace Officers⁵ (Registry) is a list of all persons appointed to police officer or peace officer titles within New York State. Police and peace officer employers are required to submit annual employment reports to OPS by January 15th of each year. The annual reports contain the name, date of birth, social security number, rank or title, work status (full or part-time), employer, and date of successful completion of mandated basic training for each officer⁶. In addition to the annual report, whenever a police officer or peace officer is newly appointed to an organization, experiences a change in personal information, work status, or ceases to serve, the employer must notify OPS as such changes occur.

In 2013, OPS staff processed 19,741 Registry transactions. As of June 1, 2014 there were 2,377 police and peace officer employers consisting of 170,934 active personnel as well as legacy data for over 600,000 former police and peace officers.

Attendant to its training and registry functions, OPS staff responds to various inquiries ranging from Freedom of Information Requests to requests from record holders for transcripts. These documents are created using third party software and exported to Portable Document Format and retained in digital format. Responses are disseminated via email. In 2013, staff responded to 2,851 requests for information, the majority of which were from record holders seeking copies of completed course work or employment histories.

The Security Guard Program

The New York State Security Guard Program is a bi-agency partnership between DCJS and the NYS Department of State (DOS). DCJS' Commissioner OPS certifies the training component of the program⁷, while DOS manages the licensure of "security guards"⁸.

Among its duties, OPS: prescribes minimum requirements for mandated training courses for security guards; approves and certifies security guard training schools, programs and

⁵ Executive Law § 845.

⁶ Article 6-A of the Public Officers Law (POL) is referred to as the Personal Privacy Protection Law. It recognizes that certain agencies, including DCJS, may maintain "personal information" as part of a "public safety agency record". See POL § 92 as to pertinent definitional terms. Accordingly, DCJS collects DOB and SSN as part of a public safety agency record. This data is considered "relevant and necessary," in accordance with POL § 94, to accomplishing DCJS' statutory training duties.

⁷ General Business Law (GBL) § 89-n, Executive Law §§, 841-b, and 841-c.

⁸ See GBL § 89-f for definition of term "security guards" and GBL § 89-n with respect to more detail regarding DOS training requirements.

courses which meet or exceed the minimum requirements and issues certificates of approval to such schools; certifies security guard instructors and issues appropriate certificates; and records satisfactory completion of such courses by security guards or applicants.

The approval of security guard schools and instructors follows a model similar to that of that used in certifying police and peace officers; however, unlike the police and peace officer community, security guard Training schools are private, for-profit entities approved by DCJS.

The current model for recording successful completion of security guard courses training utilizes Optical Mark Reader forms completed by the students and submitted by the school director. OPS staff utilizes a Pearson Op-Scan to collect the student data from the schools. The current system uses Object Linking and Embedding (OLE) technology to capture the underlying data. The data is then converted to a flat-file format for import into the database and for export to DOS.

In 2013, OPS monitored approximately 500 security guard schools, 2000 security guard instructors, and recorded completion of training programs for 212,382 security guard students.

1.3 Current Public Safety Credentialing and Training System (PSCTS) Description

The current process for collecting, maintaining and recording data, and certifying training programs and personnel consists of a blend of applications centered on an Ingenium user interface installed in 1999 . The current system no longer meets the needs of DCJS and requires the use of additional software products such as Crystal Reports and Microsoft Excel to provide meaningful data reporting, generate certificates, course approval letters, record course completion data, and track performance measures. Any documentation received or transmitted by OPS staff is maintained in multiple locations on agency servers and is not accessible to all staff.

A significant component of the first project to be undertaken under this RFP will include consolidation of functionality from multiple software products and file locations to a single tool capable of recording and maintaining data, storing files and communications, as well as delivering, monitoring and recording completion of on-line training programs.

1.4 The Future System – First Project to be undertaken under this RFP

DCJS is seeking to procure an internet-based user interface designed to manage certifications, personnel, curricula, and online learning in the public safety arena. The system must provide a secure environment for DCJS staff and our customers to: maintain a police and peace officer registry; manage the curriculum approval process; maintain

course content and lesson plans; manage instructor certification; administer personnel changes and organizational histories; record completion of mandated and voluntary training programs; produce statistical reports on student performance; distribute and analyze evaluation instruments; attach or link to relevant documentation; and create and distribute pre-designed and ad-hoc reporting.

It is critical that the future system have the following capabilities, as further described throughout this RFP;

- A. Assists DCJS and employers of peace officers and police officers in determining if there is noncompliance with applicable state law(s) and/or regulation(s) by providing automated analysis of gaps or deficiencies in mandated training qualifications and employment histories.
- B. Utilizes a secure connection to provide a monitored self-service model where the majority of transactions are entered by the course director, security guard school director, and/or the employer and allow approval by DCJS staff before being finalized.
- C. Allows expansion of access to other public safety agencies to provide for their responsibilities with respect to credentialing and training of public safety personnel.
- D. A scalable system that will meet anticipated growth of 10% per year.
- E. System is capable of encompassing a fully functional Learning Management System (LMS) in the event that NYS wishes to develop and deliver on-line content using said system in the future.

2.0 Administrative Requirements and Information

2.1 Information to be Communicated in Writing or by E-mail from NYS

All Proposals submitted in response to this RFP and all Questions, Communications and Submissions to NYS must be written in the English Language with quantities expressed using Arabic numerals. All Prices shall be expressed, and all payments shall be made, in United States Dollars (\$ USD). Any proposal or submission received that does not meet the above criteria may be rejected at the sole option of NYS.

NYS shall provide all information, responses to questions and communications concerning the solicitation in writing or by electronic mail to all vendors as required by this RFP. Such information will include, but may not be limited to, answers to Offerer inquiries; RFP clarifications and amendments; clarification of Process rules and Evaluation criteria. NYS has established a link to the PSCTS webpage for the purpose of disseminating information relating to this procurement and vendors are encouraged to monitor this webpage. The webpage URL is provided on the cover page of this RFP.

2.2 Submission of Written Questions

Any questions related to this RFP or requests for clarification, must be submitted via electronic mail to the NYS Sole Designated Contact by the date and time specified in the Calendar of Events. **Neither phone nor fax inquires will be accepted.**

The submission must cite the particular page, section and paragraph number, where applicable. NYS has provided a Questions Template form, Attachment 1, which provides the format/content vendors shall use in submitting questions by electronic mail regarding this RFP. The questions shall be attached to the electronic mail as Microsoft Word documents or as Excel Spreadsheets at a Microsoft Office 2010 or higher level.

Note: Vendors are encouraged to submit questions as early and often as necessary during the Question and Answer period, but no later than the deadline for submission of vendor's questions specified in the Calendar of Events. NYS will make every effort to respond to questions as quickly as possible.

2.3 Issuance of Official Responses to Vendors' Questions

All questions and answers will be distributed to all vendors that submit questions related to this RFP via electronic mail by the NYS Sole Designated Contact. The final Question and Answer document will be posted, on or about the date specified in the Calendar of Events on the website established for the purpose of disseminating information relating to this procurement and vendors are encouraged to monitor this website. The website URL is provided on the cover page of this RFP.

2.4 Delivery of Proposals

All Bid Proposals must be submitted so that they are received by the NYS Sole Designated Procurement Contact at the address specified on the cover page of this RFP by the date and time specified in the Calendar of Events. All Bid Proposals must be organized and submitted in two parts: (1) a Technical Proposal and (2) a Financial/Administrative Proposal, each of which will be evaluated separately. Therefore, each part must be bound and packaged in separate, sealed and labeled envelopes/containers and clearly identified as to contents (e.g., Technical Proposal or Financial/Administrative Proposal).

All Bids must have a label on the outside of the package or shipping container with the following information:

BID ENCLOSED Project Code – CJS 2014-01

Public Safety Credentialing and Training System

DO NOT OPEN UNTIL September 29, 2014; 4:00 pm

Faxed proposals and electronic submission will not be accepted. Proposals received by the State after the proposal due date and time specified in the Calendar of Events will be refused. If proposal packaging labels are not sufficient to identify the contents, NYS reserves the right to open packages for the purpose of identifying the source and contents of the package. All materials submitted by the Bidder become the property of the State of New York Division of Criminal Justice Services and may be returned only at the sole discretion of NYS.

2.5 Proposal Format and Content Requirements

Offerers must submit a complete response to this RFP in conformance with the format, content and administrative requirements set forth below. The Offerer's response to this RFP must be submitted as two separately bound and identified proposals the first of which is the Technical Proposal and the second is the Financial/Administrative Proposal. The two packages must contain the following information. Failure to submit all of the following information may render the Offerer's proposal non responsive. Minor omissions deemed not critical may be corrected at the sole discretion of the State.

Table of Contents: Each package must include a Table of Contents.

Index Tabs: Each major section of the proposal must be labeled with an index tab that completely identifies the title of the major section as it is named in the mandatory Table of Contents.

Page Numbering: Each page of the proposal must be dated and numbered consecutively within each section submitted by the Offerer.

A. Package 1 - Technical Proposal

The Offerer must submit 8 bound paper copies, 1 of which must contain original notarized signatures, of their Technical Proposal. The Offerer must also submit one complete electronic version of the Technical Proposal on PC Compatible Windows Readable CD-ROM saved as in Adobe Acrobat® pdf format. Originally signed documents and drawings may be provided in Adobe Acrobat® pdf format, provided that the Offerer has submitted the documents containing the original signature elsewhere in its submission. Separate CD-ROM submissions must be made for the Technical and for the Financial/Administrative Proposals. Do not include information/files from the Financial/Administrative Proposal or any Cost Data in the paper copies or on the CD-ROM which contains the Technical Proposal.

The items which must be included in the Technical Proposal properly completed, signed and notarized, where appropriate, are listed below:

1. One (1) original paper copy of the Technical Proposal with original notarized signatures.
2. Seven (7) paper copies of the Technical Proposal in addition to the one (1) original from (1) above.
3. One (1) complete electronic version of the Technical Proposal on a PC Compatible Windows CD-ROM saved in Adobe Acrobat® pdf format.
4. Offerer Firm Information Form, Attachment 5 (this document also required in Financial/Administrative Proposal).
5. An Executive Summary that includes all of the items and addresses all of the elements specified in Subsection 3.1.A. The narrative portion of the executive summary is limited to ten (10) pages, exclusive of attachments (such as the DUNS and SEC reports).
6. At least two (2) Completed Mandatory Qualifying Experience Customer Reference Forms, Attachment 6, as further specified in Section 3.B
7. Mandatory Base System Requirements – COTS or Customized, Attachment 7.
8. Optional Features – COTS or Customized, Attachment 7a.
9. Mandatory Base System Requirements – Solution and/or Documentation Descriptions with Forms Required for Offerer Bid Response, Attachment 8.
10. Project Plan (that includes all of the items and addresses all of the elements specified in Subsection 3.1.D).
11. Signed & Completed Proposed Subcontractors, Attachment 18.

B. Package 2 – Financial/Administrative Proposal

The Offerer must submit 8 bound paper copies, 1 of which must contain original notarized signatures, of their Financial/Administrative Proposal. The Offerer must also submit one complete electronic version of the Financial/Administrative Proposal on a PC

Compatible Windows CD-ROM saved in Adobe Acrobat® pdf format. Originally signed documents and drawings may be provided in Adobe Acrobat® pdf format, provided that the Offerer has submitted the documents containing the original signature elsewhere in its submission. Separate CD-ROM submissions must be made for the Technical Proposal and the Financial/Administrative Proposal. Do not include information/files from the Technical Proposal in the paper copies or on the CD-ROM which contains the Financial/Administrative Proposal.

The items which must be included in the Financial/Administrative Proposal properly completed, signed and notarized, where appropriate are listed below:

1. One (1) original paper copy of the Financial/Administrative Proposal with original notarized signatures.
2. Seven (7) paper copies of the Financial/Administrative Proposal in addition to the one (1) original from (1) above.
3. One (1) complete electronic version of the Financial/Administrative Proposal on a PC Compatible Windows CD-ROM saved in Adobe Acrobat® pdf format.
4. Signed, notarized and completed NYS Non-Disclosure Agreement, for bidder and each sub-contractor, Attachment 2.
5. Completed Offerer Firm Information Form, Attachment 5 (same as for Technical Proposal).
6. Completed and signed Staffing Plan, Attachment 9
7. Completed and signed MWBE Utilization Plan, Attachment 10
8. Signed & Completed Firm Offer Letter and Conflict of Interest Disclosure, enclose Resolution of the Corporate Board of Directors, where applicable (pursuant to RFP Subsection 3.3), Attachment 11.
9. Signed & Completed Non-Discrimination in Employment in Northern Ireland Statement, Attachment 12.
10. Signed & Completed Non-Collusive Bidding Certification, Attachment 13.
11. Signed & Completed NYS Procurement Lobbying Forms 1, 2 and 3, Attachment 14.
12. Signed & Completed N.Y.S. Department of Taxation and Finance Contractor Certification to Covered Agency Form ST-220-CA, Attachment 15.
13. Signed & Completed NYS Standard Vendor Responsibility Questionnaire, Attachment 16 or file the Vendor Responsibility Questionnaire online via the New York State VendRep System.
14. Completed Encouraging Use of New York State Businesses in Contract Performance, Attachment 17.
15. Signed & Completed Proposed Subcontractors, Attachment 18.
16. Signed & Completed Key Subcontractor Certification, Attachment 19 for each key subcontractor proposed by the Offerer.
17. Signed & Completed State Consultant Services Contractor's Annual Employment Report , Attachment 21.
18. Signed & Completed FBI CJIS Security Addendum for bidder and each sub-contractor, Attachment 22.
19. Completed Attachment 23 Proposed Fixed Purchase Price - Mandatory Base System.
20. Completed Attachment 24 Maintenance and Support Price - Mandatory Base System.

- 21. Completed Attachment 25 Optional Licensing and Professional Services Price List. Completed Attachment 26 Total Proposed Cost for Offerer's Mandatory Base system for Initial 10 Year Contract Period.
- 22. Completed Attachment 27 Proposed Fixed-Price Milestone Deliverable Payment Schedule.
- 23. Completed Attachment 28 Detailed Optional Features Price List
- 24. Completed Attachment 29 Optional Services Price List

2.6 Mandatory Requirement - No Exceptions Permitted

No exceptions to any requirement of this RFP are permitted. Proposals of Offerers taking exceptions, reservations or otherwise qualifying or limiting any submission will be deemed non-responsive. Requirement of this RFP means all requirements contained herein and as may later be identified or amended by NYS on notice to vendors via the website established for the purpose of disseminating information relating to this procurement.

2.7 NYS Reserves the Right to Modify Requirements

NYS reserves the right to modify the requirements of this procurement and RFP and to modify, correct and clarify requirements at any time provided that modifications would not materially benefit or disadvantage an Offerer.

2.8 Costs Incurred Prior to Contract Approval

The State of New York and DCJS are not liable for any cost incurred by an Offerer in preparation for, or prior to, the approval of an executed contract by the Attorney General and the Office of the State Comptroller. No cost will be incurred by NYS for the offer's or prospective Offerer's participation in any pre-contract award activity. Submission of response to this RFP shall not be construed as a commitment by the State to proceed with this project.

2.9 Mandatory Requirement - Price Protection

The Offerer agrees that all of the prices, terms, warranties and benefits established in the Agreement are comparable to or better than the equivalent terms being offered by the vendor to other customers using similar scope and volume of services. If the Offerer shall, during the term of this Agreement, enter into arrangements with any other customer providing greater benefits or more favorable terms, the Contract shall thereupon be deemed amended to provide the same to the State.

2.10 Procurement Record

NYS shall maintain a Procurement Record which documents all decisions regarding the procurement process, particularly the quantification of criteria used to determine an award based on best value; or where not quantifiable, the justification which demonstrates that best value will be achieved pursuant to State Finance Law § 163(9)(g). The Procurement Record will be forwarded to the Office of the State Comptroller and as applicable to the Office of the Attorney General (Department of Law) in support of their respective evaluation activity.

2.11 Notification of Award and Opportunity for Debriefing

The successful Offerer will be advised of selection by NYS through the issuance of a formal written correspondence indicating a proposed award. All Offerers will be notified of the selection or rejection of their proposals. Once an award has been made, Offerers may submit a written request for a debriefing as to why their proposal did not result in an award. The written request must be received by the NYS Sole Designated Contact identified on the cover page of this RFP no later than ten (10) business days from the date of the award announcement.

2.12 DCJS Contract Award Protest Procedure

DCJS strives to assure a fair, open and competitive process to all vendors qualified to respond to this Procurement. In the event that any vendor has a complaint or objection to the RFP requirements, the procurement process or any matter affecting the submission of a vendor's Bid Proposal, the vendor is encouraged to informally contact the NYS Sole Designated Contact for this procurement, listed on the cover page of this RFP, immediately to resolve the matter.

If the vendor believes that the objection affects the outcome or nature of the proposed award for this Procurement, the vendor must follow the procedures for timely filing a formal protest set forth in the NYS Contract Award Protest Procedures at Appendix H of this RFP by the deadline set forth in the procedure. Prior to Contract award, protests which may affect the outcome or nature of the award may only be considered by the State in the context of a formal written protest filed in accordance with the procedure at Appendix H.

2.13 State's Reserved Rights

This is a best value procurement. NYS and the State of New York intend to acquire goods and services that represent the "best value." NYS reserves the right to:

- a. At any time prior to contract execution withdraw or award the RFP in whole or in part;
- b. At any time prior to contract execution, accept or reject any and all Proposals, or separable portions of Proposals, and waive minor irregularities and/or omissions in Proposals if the State determines the best interests of the State will be served;
- c. In its sole discretion, accept or reject illegible, incomplete, or vague bids, and its decision shall be final;
- d. During the evaluation process, at its sole option, seek clarification from an Offerer for the purpose of assuring NYS's full understanding of the Offerer's responsiveness to the RFP requirements. This clarification information, if required in writing by NYS, must be submitted in writing in accordance with the formats as prescribed by NYS at the time it is requested by NYS, and if received by the due date requested, shall be included as a formal part of the Offerer's Proposal. Failure to provide required information by the specified due date may result in rejection of the Offerer's Proposal. Bidders may be required to participate in individual presentations. Presentations and clarification information provided pursuant to a request by NYS if any will be considered in the evaluation process;
- e. Eliminate mandatory requirements if deemed to be in the State's best interests, or negotiate additional terms and conditions in any resulting Contract that are to the State's advantage;
- f. Amend the RFP if it becomes necessary in the sole discretion of NYS, and in such an event addenda will be provided by NYS to all Bidders.
- g. Establish evaluation criteria relating to quality, quantity, performance and cost; establish the relative importance of each criterion; and evaluate proposals as well as award contracts on the basis of these criteria. As a result, service and technology procurements administered through an RFP process would not necessarily be awarded to the responsible Offerer submitting the lowest priced proposal pursuant to State Finance Law §§ 163(4)(d), (7) and (9)(b));
- h. Award a contract for any or all parts of a proposal and negotiate contract terms and conditions to meet agency program requirements consistent with the solicitation;
- i. Consider all Offerers' proposals firm and binding for a period of at least twelve (12) months from the Bid Proposal Due date, or until such time as a Contract resulting from this RFP is approved by the NYS Comptroller. In the event that a contract is not approved by the Office of the State Comptroller within twelve (12) months Bidder offers shall remain firm and binding until a contract is approved by OSC, unless the Bidder delivers to NYS written notice of withdrawal of its proposal after the twelve (12) month period has passed;
- j. Establish that in the event two proposals are found to be substantially equivalent, price shall be the basis for determining the award recipient or, when price and other factors are found to be substantially equivalent, the determination of the agency head or designee to award a contract to one Offerer shall be final. The basis for determining the award shall be documented in the Procurement Record;
- k. Elect to award a contract to a responsive and responsible Offerers, provided that the basis for the election at the time of purchase shall be the most practical and economical alternative and shall be in the best interests of the State

2.14 Contract Term

The Contract awarded in this procurement shall not be deemed executed unless and until it shall have been approved by the Attorney General of the State of New York and the Comptroller of the State of New York or their respective staff designated for that purpose.

The Contract shall commence upon the date of its approval by the New York State Comptroller (“Effective Date”) and shall continue for a period of ten (10) years with the option to renew. NYS reserves the right to renew the agreement, in whole or in part, for two additional five (5) year terms upon the conditions and at the rates set forth in the Contract or subsequent amendments, and as afforded by the cost of living index. Except as established in Price Protection, Subsection 2.9 (as negotiated), the Contract will be subject to amendment only upon mutual written agreement of the parties, which agreement must be approved by the Attorney General and the Comptroller of the State of New York. The State shall have the right to renegotiate the terms and conditions of the Contract in the event applicable State or Federal law, policy, rules, regulations and guidelines are altered from those existing at the time of the original contract in order to be in continuous compliance therewith.

2.15 Time is of the Essence

Contractor understands that prompt performance of all services and delivery hereunder is required by NYS in order to meet its schedule of commitments, statutory purpose. Time is of the essence in the resulting Contract and will be a substantial and a material term of the Contract. In the event of any anticipated or actual delays in meeting deadlines or scheduled completion dates, Contractor shall provide additional personnel, software, hardware or any other resource deemed beneficial as required and at no additional charge to NYS, in order to complete the project in a timely manner.

Notwithstanding the above, any dates or times at which Contractor is required to make specified performance under the contract, the time and dates may be postponed to the extent that Contractor is prevented from meeting such dates or times by NYS or by causes beyond Contractor’s reasonable control. Any and all extensions must be agreed to in writing by the parties.

2.16 Contract Formation

The Contract will incorporate this RFP, any Exhibits, all Appendices, all Attachments, all submissions, the Offerer’s Bid Proposal, clarifications and additional information issued by NYS during the course of this procurement and additional terms which may be agreed to by the parties in writing. Execution by the successful Offerer shall not be deemed final until the execution of the Contract. The Contract will be deemed executed upon, and will

not be considered fully executed and binding until, receipt of approval by the Attorney General of the State of New York and the Comptroller of the State of New York or members of their staff designated by them for that purpose.

The State reserves the right to renegotiate the terms and conditions of the Contract in the event that applicable New York State or Federal laws, statutes, rules, regulations, policies and/or guidelines are altered from those existing at the time the Contract is approved by the Comptroller so that NYS will be in continuous compliance therewith. The Contract is subject to amendment only upon the mutual written agreement of the Parties, which agreement must be approved by the Comptroller.

The successful applicant will be required to timely enter into a contract with NYS related to service delivery within ten (10) business days of notification and receipt of the final contract. Attachment 20 is a draft contract of terms and conditions, some of which cannot be changed (i.e. *Appendix A: Standard Clauses for New York State Contracts*). The final contract may contain new or amended contractual provisions. NYS reserves the right to negotiate minor terms and conditions relative to the RFP and the applicant's response to meet agency program requirements consistent with the solicitation.

During contract execution, the State expects to have direct access to Offerer personnel who have full authority to make commitments on behalf of the Offerer. Any contract must conform to the laws of New York State.

2.17 Mandatory Requirement - Standard Clauses for New York State Contracts

- A. The parties agree that this contract is governed by and incorporates all of the terms and conditions of the document identified as Appendix A – Standard Clauses for New York State Contracts dated January 2014 annexed hereto and which is incorporated into this Contract as though fully set forth in its entirety herein.
- B. The parties shall agree to and/or accept all items and conditions as specified within the following Appendices and/or other attachments annexed to this Agreement:
 - Any Change Request Order Form (Appendix J) which is subsequently mutually entered into with respect to services during the terms of this Agreement;
 - Any Statement of Work (SOW) issued by NYS to the Contractor under the terms of this Agreement from time to time;
 - OSC Consultant Contractor Services Form A and Form B Addendum (Appendix E);
 - MacBride Fair Employment – Northern Ireland Non-Discrimination (Attachment 12);
 - Non Collusive Bidding Certification (State Finance Law Section 139-d) (Attachment 13);
 - NYS Procurement Lobbying Guidelines (Attachment 14);

- State Finance Law Sections 139-j and 139-k Affirmation (Attachment 14, Form 3)
- Affirmation of Understanding and Agreement pursuant to State Finance Law §139-j (3) and §139-j (6) (b) (Attachment 14, Form 1)
- Disclosure of Prior Non Responsibility Determination (Attachment 14, Form 2)
- Workers Compensation coverage certificate
- Proof of Disability Benefits Insurance
- OR Form CE-200 from Workers Compensation demonstrating relief from Workers Compensation/Disability (see www.wcb.ny.gov)
- Minority and Women-Owned Business Enterprise (MWBE) and Equal Opportunities Requirements.
- The NYS Public Safety Credentialing and Training System (PSCTS) Request For Proposals (RFP), dated August 29, 2014, including all RFP appendices
- Contractor's RFP Submission and any Contractor response to inquiries relating thereto.

2.18 Mandatory Requirement for Contracts Estimated to be \$1,000,000 or More:

- a. Subsequent to the award of procurement contracts in an amount estimated to be \$1,000,000 or more, the Contractor will be required to document their efforts to encourage the participation of New York State business enterprises as suppliers and subcontractors by showing they have (i) solicited bids in a timely and adequate manner from New York State business enterprises including certified minority-owned businesses, (ii) contacted the New York State Department of Economic Development to obtain listings of New York State business enterprises, (iii) placed notices for subcontractors and suppliers in newspapers, journals or other trade publications distributed in New York State, or (iv) participated in contractor outreach conferences. If the Contractor determines that New York State business enterprises are not available to participate on the contract as subcontractors or suppliers, the Contractor shall provide a statement indicating the method by which such determination was made. If the Contractor does not intend to use subcontractors, the Contractor shall provide a statement verifying such.
- b. Subsequent to the award of procurement contracts in the amount estimated to be \$1,000,000 or more, contractors will be required to notify New York State residents of employment opportunities through listing any such positions with the Community Services Division of the New York State Department of Labor, or providing for such notifications in a manner as is consistent with existing collective bargaining contracts or agreements.

- c. Offerers located in a foreign country are notified that the State may assign or otherwise transfer offset credits created by any procurement contract of \$1,000,000 or more to third parties located in New York State, and that Offerers shall be obligated to cooperate with the State in any and all respects in making such assignment or transfer, including, but not limited to, executing any and all documents deemed by the State to be necessary or desirable to effectuate such assignment or transfer, and using their best efforts to obtain the recognition and accession to such assignment or transfer by any applicable foreign government.

2.19 Encouraging Use of New York State Businesses in Contract Performance

New York State businesses have a substantial presence in State contracts and strongly contribute to the economies of the state and the nation. In recognition of their economic activity and leadership in doing business in New York State, bidders are strongly encouraged and expected to consider New York State businesses in the fulfillment of the requirements of the contract(s) resulting from this RFP. Such partnering with New York State businesses may be as subcontractors, suppliers, protégés or other supporting roles.

To assist in demonstrating commitment to the use of New York State businesses in the performance of the contract(s), all bidders must complete the form provided in RFP Attachment 17 (Encouraging Use of New York State Businesses in Contract Performance).

2.20 Mandatory Requirement - Discriminatory Jurisdictions

Offerers are hereby notified that state agencies and authorities are prohibited from entering into contracts with businesses whose principal place of business is located in a discriminatory jurisdiction. Discriminatory jurisdiction is defined as a state or political subdivision which employs a preference or price distorting mechanism to the detriment of or otherwise discriminates against a New York State business enterprise in the procurement of commodities and services by the same or a non-governmental entity influenced by the same. A list of discriminatory jurisdictions is maintained by the commissioner of the New York State Department of Economic Development.

2.21 Negotiations with the Next Highest Offerer

In the event that NYS should be unsuccessful in finalizing a contract within thirty (30) business days following the date of the notice of award with the originally selected Offerer, NYS may at any time following the sixtieth business day at its option begin

negotiations with the next highest scored Offerer and in such an event NYS will give notice to all Offerers that it has done so.

2.22 Prime Contractor

Offerer is required to serve as the Prime Contractor for this project and is referred to hereafter as "Contractor." The Contractor is responsible for meeting all Contract obligations set forth in the solicitation and Contract, including all Appendices, Attachments, Exhibits, and any subsequent amendments mutually agreed to in writing between the parties. The Contractor is responsible for payment of all subcontractors and suppliers, including all third-party equipment and service providers contracted by or through the Contractor in performance of the agreement. Where equipment or services are supplied by or through the Contractor under the Contract, Contractor must assume full integration responsibility for delivery, installation, maintenance, performance, and warranty support services for such items. The Contractor shall also be responsible for payment of any license fees, or other monies due to employees, subcontractors and/or others in connection with services delivered by the Contractor with respect to this Contract. It shall be the responsibility of the Contractor throughout the Contract term, to have appropriate staff available to communicate and/or otherwise meet with NYS, as may be determined necessary by NYS to provide design development, Contractor service updates, confer on technical aspects of product, specific Contractor service delivery activities, and to target specific issues and clarify and/or address any conversion or other implementation problems regarding the PSCTS. Such communication may be through phone calls and/or emails and meetings through videoconferences or conference calls unless NYS determines it necessary for formal written communication and face-to-face meetings.

It is understood and agreed that the legal status of the Contractor, its agents, officers and employees under the Contract is that of an independent contractor, and in no manner shall they be deemed employees of the State, or of NYS, and therefore they are not entitled to any of the benefits associated with such employment. The Contractor agrees, during the term of the Contract, to maintain, at Contractor's expense, those benefits to which its employees would otherwise be entitled by law, including health benefits, and all necessary insurance for its employees, including workers' compensation, disability, and unemployment insurance, and to provide the State with certification of such insurance upon request. The Contractor remains responsible for all applicable federal, state, and local taxes, and all FICA contributions.

2.23 Subcontractors

Offerers may submit proposals that include subcontractors. All subcontractors proposed by the Offerer must be identified in the proposal and must be acceptable to NYS. The Offerer as Contractor remains the single point of contact for NYS. NYS will contract with only the Contractor. Where applicable, for example in the Project Plan section of the Offerer's proposal, the specific subcontractor proposed to perform the Contractor's obligation must be identified, but such identification does not relieve the Contractor of any responsibility for performance under the contract with NYS. All subcontractors will be required to execute confidentiality agreements and non-disclosure agreements. NYS reserves the right to require fingerprint (which shall be at Contractor's or the Subcontractor's expense) and security background checks of subcontractor personnel providing services to the Contractor in connection with this RFP and the resulting Contract. Additionally, in recognition of the critical public safety nature of the PSCTS to preservation of the health, safety and welfare of the citizens of the State, all subcontracts must contain an express provision that the subcontract is not further assignable or transferable without the written consent of the New York State Comptroller.

Offerer must, in its bid proposal, identify the name of each proposed subcontractor on Attachment 18 *Proposed Subcontractors* and provide a completed and signed Attachment 19 *Key Subcontractor Certification* for each key subcontractor (as defined in the Glossary – Appendix S) proposed by the Offerer. The Contractor is required to include in all subcontracts the affirmative obligation of all previously approved subcontractors to disclose to Contractor and to the State any material change to the information disclosed in Attachment 19 *Key Subcontractor Certification* that occurs after bid submission and during the Contract term. The State shall have the right to prospectively cancel the Contract, in whole or in part, for cause if it finds that such change materially adversely affects the best interests of the State.

NYS reserves the right to require the Offerer to have executed Contracts with all proposed key subcontractors prior to Contract award, and may withhold or withdraw approval of the proposed award in the event that such agreements have not been entered into within a reasonable time to allow timely Contract award, such timeliness to be determined solely by NYS.

As a condition of Contract award and thereafter throughout the Contract term, the Successful Offerer shall furnish a written copy of all subcontracts, including subsequent amendments thereto, to the State and certify the completeness thereof of all executed subcontracts or third-party agreements, which support the Contractor's ability to furnish the products and services for this project. In the context of this section, the phrases "certify the completeness thereof" and "certify the terms of third party agreements" shall mean that the Contractor has fully disclosed all terms and conditions of the aforesaid subcontracts and/or third party agreements and will affirmatively disclose to the State any

amendments thereto which occur subsequent to the certification. The State's failure to receive or request such agreements shall not constitute a waiver of these rights.

Additionally, to the extent that the Contractor identifies as a proposed subcontractor in its' proposal or under this PSCTS Contract an entity which has independently executed a contract with the State of New York for similar services or products as those to be provided through Contractor under this PSCTS Contract, and such subcontractor's direct State contract imposes obligations, terms or conditions on the subcontractor which are more beneficial to the State than those set forth in the Contract resulting from this procurement as to such subcontractor's responsibilities under the PSCTS, the State reserves the right to:

- a. require the Contractor to incorporate into the PSCTS Contract such more beneficial terms and conditions, and
- b. require the Contractor to deliver to NYS the subcontractor's written agreement to incorporate and honor such additional or beneficial terms to its obligations to NYS under the PSCTS Contract, and
- c. withhold the approval of subcontractor pending receipt by NYS of written agreements complying with a and b, above.

In the alternative, NYS reserves the right to delete any portion of work to be performed by such subcontractor from the scope of the PSCTS and to acquire such services under the independent State contract where the State determines it would be more advantageous to acquire such products or services directly.

2.24 Trade Secret Materials

Proposals and supporting material submitted to NYS in response to this RFP are subject to the Freedom of Information Law (Public Officers Law, Article 6; hereinafter FOIL). Pursuant to section 87(2) of FOIL, records or portions thereof that "are trade secrets or are submitted to an agency by a commercial enterprise or derived from information from a commercial enterprise and which if disclosed would cause substantial injury to the competitive position of the subject enterprise" may be exempt from disclosure. In addition, pursuant to section 89(5)(a)(1-a) of FOIL, records or portions thereof that contain critical infrastructure information may be exempt from disclosure ("critical infrastructure" is defined in sections 86(5) of FOIL). An Offerer must follow the procedures below, if it intends to seek an exemption from disclosure under FOIL of either or both types of material. Where such claimed material is embedded in the Bid Proposal, it shall be the responsibility of the Offerer, at its sole cost and expense, to submit redacted versions of the Bid Proposal within ten (10) days of a request by the State.

Trade secret or proprietary materials or critical infrastructure information as defined by the laws of the State of New York must be clearly marked and identified as such by the Offerer upon submission. Offerers intending to seek an exemption from disclosure of claimed trade secret or proprietary materials or claimed critical infrastructure information under FOIL must, at time of submission, request the exemption in writing and provide an explanation of (i) why the disclosure of the identified information would cause substantial injury to the competitive position of the Offerer, or (ii) why the information constitutes critical infrastructure information which should be exempted from disclosure pursuant to section 87(2) of the Public Officers Law. Acceptance of the identified information by the State does not constitute a determination that the information is exempt from disclosure under FOIL. Determinations as to whether the materials or information may be withheld from disclosure will be made in accordance with FOIL at the time a request for such information is received by the State.

3.0 Specifications for Evaluation

Proposals submitted in response to this RFP must meet all of the requirements established by NYS for this procurement, including the requirements of this RFP and any subsequent information and communication released by NYS to Offerers, and any other communication made by NYS pursuant to the terms of this RFP. Proposals which fail to meet all of the mandatory requirements will be deemed non-responsive and will not be further evaluated by NYS. Submission of a proposal is a representation to NYS that the Offerer is capable of meeting all mandatory requirements of the procurement within the required timeframes.

3.1 Technical Specifications

A. Executive Summary

Each Offerer must submit an executive summary of its proposal. Offerers should utilize this section to demonstrate how its overall proposal, specific solution and implementation approach meet NYS business objectives as defined in this RFP.

The executive summary shall address, at a minimum:

1. The executive commitment of the Offerer, including the responsible executives and a description of their responsibilities in the organization and in this particular procurement. Include, at a minimum:
 - a. Involvement of the Offerers' executive team in this project;
 - b. How many other large projects within the Offerers' organization that would be concurrent with this project;
 - c. How the Offerers' executive team is made aware of issues within a project (e.g., QA process);
 - d. Escalation process from the Offerers' Project Manager up to the executive team; and
 - e. Proposed project steering committee membership, meeting frequency, etc.
2. The Offerer's strategic direction, ongoing commitment to research and development and plans for future product(s) that may affect the NYS programs required herein including, at a minimum, what the current schedule looks like for new releases / versions through the next five (5) years with an outline of new or enhanced major features by release / version. Include, at a minimum:

- a. Commitment to the product(s) being proposed as the solution for NYS;
 - b. Publicly proposed plans or strategies under evaluation for the acquisition, merger or other restructuring of the organization or that of any proposed subcontractor;
 - c. How systems fit into the Offerers' product and service portfolio;
 - d. How the proposed solution positions NYS for the next generation of system capabilities;
 - e. A roadmap of the next five (5) years for the Offerers' organization for its products and services; and
 - f. How industry and open standards are utilized in the Offerers' proposed solution.
3. Conceptual overview of the solution that is being proposed for NYS. Include, at a minimum:
 - a. Hardware and software solution including scalability during the contract term;
 - b. Conversion of legacy data and implementation plans;
 - c. Satisfying accuracy requirements;
 - d. How the Offerer's experience with implementing similar, large-scale systems positions the Offerer for a successful delivery to NYS.
4. The Offerer's scope of installed sites including, but not limited to, the following:
 - a. The number of Public Safety Credentialing and Training Systems installed, by product version, and in production throughout the world, by country and state within the U.S.;
 - b. The number of these systems that have been installed within the past five (5) years, by product version;
 - c. Supports a minimum of 150 concurrent users;
 - d. The number of these systems that are installed with database sizes of at least fifty thousand (50,000) personnel records and one hundred thousand (100,000) transactions annually, by product version; and
 - e. A brief discussion of the result of the engagement with each customer referenced in Section 3.1.B.
5. The following business information:
 - a. Delineation of the Offerer's form of organization and structure, including ownership and control, financing structure and any existing options, rights and warranties, shelf registration and other form of encumbrance or pledge against equity or assets;

- b. Offerer's DUNS identifier;
- c. Copy of the Offerer's most current Dun and Bradstreet report;
- d. Copy of the Offerer's most recent SEC 10 or equivalent filing; and
- e. Disclosure of active investigations of the Offerer or of any holding company of which the Offerer is a subsidiary by any exchange or governmental entity which would not necessarily result in disapproval of the proposed agreement, but must be disclosed.

Offerers are advised that for contracts submitted for approval under the New York State Finance Law ("Section 112 approval"), the State Comptroller may independently ascertain, determine, evaluate, approve, reject or make further inquiry into the terms and conditions of the agreement and may make an independent determination of the Vendor Responsibility, requisite financial strength and stability of the Offerer, an assessment of the ability of the Offerer to perform under the terms of the agreement for the period of time specified and other factors which the Comptroller deems in the best interest of the State of New York. Determining the acceptability of an Offerer can extend to an evaluation by the Comptroller of any proposed subcontractors and if applicable, holding companies. In the course of the contract approval process, the Comptroller may submit questions and requests for further information from NYS. NYS in turn may rely on the Offerer for assistance in preparation of the responses to these inquiries, and these inquiries and responses submitted will become part of the procurement record.

B. Offerer Mandatory Qualifying Experience and Customer References

Because of the public safety importance of the PSCTS, NYS must give consideration to particular subject matter experience, including technical expertise of the Offerer and Offerer's project team, and to other factors. The Offerer must therefore, as Contractor, have experience in the successful implementation of credentialing and training system systems that meet the requirements specified in this section. Therefore, the Offerer must provide, as part of the Technical Proposal, the information required in this section to document their experience. All requested information shall be completed on the attachments referenced below.

NYS will contact all of the customer references provided by the vendor to receive the *Mandatory Qualifying Experience Customer Reference Questionnaire* contained in Appendix F.

Mandatory Qualifying Experience –Customer References

The Offerer must provide all contact information and qualifying data on Attachment 6, Mandatory *Qualifying Experience Customer Reference Form*, for a minimum of two (2) customers, organizations not controlled or owned by the Offerer, in the past five years for which the Offerer, as Contractor, has successfully implemented a PSCTS or comparable system that is currently in production for at least 90 days, currently utilizing a software release/version that is within one major release from the proposed and where all hosting services are provided by the Customer.

If all components or features listed below have not been installed at a single location Offerers may provide additional customer site references up to a maximum of seven (7) to document their experience in providing all required components or features listed in section 3.1.B, *provided that* a) the first four criteria (1. Annual Validation; 2. Gap Analysis and Validity, 3. Self Service Functionality and 4. Reporting), have been installed at one or more single location(s), and b) that all criteria have been met through one or more of the customer site references.

1. Allows employers to perform annual validation of all employment records and report the results to records management staff; employers are able to input, update, and validate details specific to each individual employed by them currently and in the past (“Annual Validation”).
2. Provides Gap Analysis of the validity and pending expirations of training certificates and/or qualifications; identifies gaps in employment service (including from one employer to another); and provides notification of pending expirations of certificates and/or qualifications to employers, individual record holder(s) and records management staff (“Gap Analysis and Validity”).
3. Provides self-service functionality for employees (view access for records and certificates), employers (records and data management), training instructors and academies (training record management), and administration (configuration), application is user friendly to the average non-technical individual (“Self Service Functionality”).
4. System generates standard reports and statistics, including gap analysis; performs audits of training certificates and actions of system users; and the ability to define and generate ad hoc reports exists. Reports can be generated in standard formats including Adobe PDF and Microsoft Excel (“Reporting”).
5. Has a database of at least 50,000 personnel records and is capable of supporting 150 concurrent users; vendor support is available at a minimum Monday to Friday during business hours.
6. Performs a minimum of 100,000 transactions (records updates) annually and the application’s user interface provides feedback in 5 seconds or less, from each key press, mouse movement or other type of input or exchange.
7. System has interfaces with at least one (1) exterior agency/entity e.g. FBI, State Police, Department of Health, wherein data imports and exports occur; the interface is user friendly to the average non-technical individual and capable of self service features including bulk-upload capabilities.

8. Contains an on-line portal or equivalent component that automates processes for course enrollment, approval and completion, records management, certificate issuance; includes features including ability to approve and manage training academies, document retention and management, training course calendaring and self-service functionality for instructors and students. The system must allow NYS to upload training materials (records management) including but not limited to text files, audio files and/or video files with individual files upwards of 4GB in size. System must be capable to develop, manage, provide and administer distance learning course offerings allowing for up to 1,500 concurrent users. System must support SCORM and ASCII compliant software.

NYS may contact all the customer references by telephone or e-mail and request that they complete and return the Public Safety Credentialing and Training System Customer Reference Questionnaire as set forth in Appendix F to verify the mandatory qualifying experience, as outlined in Section 4.3.

C. First Project: Mandatory Requirement – Base Requirements for Offerer's Proposed PSCTS Solution

NYS is seeking to replace its aging Public Safety Credentialing and Training System with a new system equipped with the latest technology and software using COTS products and services, and if necessary, customized products and services. NYS has assessed the mandatory requirements for a new Public Safety Credentialing and Training System and has identified items which must be included.

In order for an Offerer's proposed PSCTS System solution to be deemed responsive to this solicitation, the solution shall meet all of the MANDATORY requirements specified in this section. As part of their Financial/Administrative Proposal, the Offerer shall submit a Firm Offer Letter, as set forth in Attachment 11, which includes a statement affirming that the Offerer's proposed PSCTS solution meets or exceeds all of the mandatory base system requirements set forth in this Section 3.1.C. As part of their Technical Proposal, the Offerer shall also complete Attachments 7, 7a and 8, as described in this section.

The Offerer's proposed Public Safety Credentialing and Training System solution shall meet all of the MANDATORY requirements specified below as well as other mandatory requirements specified in Attachments 7 and 8:

System Requirements

1. The Offerer must propose both a proven PSCTS solution and software support terms that are acceptable to NYS. The proposed support terms will enable the Offerer to fully meet all of the requirements of the RFP for the duration of the Contract and any extensions. "Proven" means that the proposed solution and provision for support have been previously placed into commerce by the Offerer, that is; the proposed solution has been procured, installed, accepted and is in operation at a level consistent with the proposed capability is within one major release of the proposed solution, for at least ninety consecutive days at an organization not owned or controlled by the Offerer, as further described in Section 3.1.B. "Support terms acceptable to NYS" means that software must be maintained so that the Offerer's proposed solution operates at or exceeds all of the requirements of this RFP. Offerer affirms its understanding that it is proposing its solution specifically to support the State's continuing public safety requirements. In the event that the Offerer discontinues the level of support offered to any of its customers operating similar products or using services and support levels similar to those provided to NYS by Offerer as Contractor for whatever reason including but not limited to obsolescence, compatibility of software, discontinuance of manufacture or other failure of Contractor's supply chain, changes in version or generation of software, or business objectives of the Offerer, such action by the Offerer does not relieve the Offerer of its obligations to the State to meet its requirements to support the software to ensure continued operation consistent within the requirements of the RFP. The parties agree that in consideration of software issues which may arise in the future, that if the Offerer discontinues marketplace offering of support of any software version similar to that installed at NYS, that Offerer shall advise NYS immediately and that NYS may in its sole discretion elect to require the Offerer's to upgrade the NYS installation at no cost to the State.
2. The proposed system must Maintain and secure Personal, Private, Sensitive Information ("PPSI") inclusive of, but not limited to dates of birth (DOB) and Social Security Numbers (SS#). The Offerer's PSCTS must be capable of utilizing a secure internet connection to safely transmit personal protected information to NYS.
3. The Offerer shall supply all software required to implement its solution including interfaces, the test environment, and technology upgrades including the Production and Test environment COTS Products.
4. The Offerer shall propose a PSCTS initially capable of processing a minimum of 100,000 personnel transactions (record updates) annually. The system shall be capable of expanding transaction capacity and records storage capacity by ten percent each subsequent year.

5. The Offerer shall propose a PSCTS capable of maintaining a training history for 1,000,000 individual training records.
6. The proposed system must be capable of vertical and horizontal scaling to allow for system expansion and initially be capable of supporting 150 concurrent users
7. Vendor support for the system will be, at a minimum 5x12 (Monday to Friday 6:00 AM to 6:00 PM)
8. The Offerer shall set up and configure a PSCTS test environment at a New York State designated facility that:
 - a. has all features and functionality of the proposed production system
 - b. is independent of and mirrors the production system
 - c. is smaller in size and capacity than the production system, but shall have all software components, providing for a test system sized to at least 5% of the production databases(s), files, and queues with comparable throughput and capacity
 - d. can be utilized by NYS staff to verify and quality assure all new vendor releases and system patches before deployment to the NYS production system
 - e. can be utilized by NYS development team to test changes in NYS software that communicates with the PSCTS.
9. Vendor will have a representative on-site for all phases of system installation.
10. The PSCTS user interface must provide feedback in less than 5 seconds after each key press, movement of the mouse, or any other physical input from the user, and after each change in the state of controls that react to input from the user, for example, displaying menus or indicating drop targets.
11. Proposed system will allow the combined records management of multiple customer separate customer populations such as the Police and Peace Officer Registry and the Security Guard Program. All populations must be capable of performing maintenance of records applicable to their assigned responsibilities. See Appendix K Table 2 Population for a list of the designated users.
12. The Offerer shall encrypt all NYS data, residing or in communication outside the NYS internal network and OTIS datacenter, with a minimum 128 AES encryption. In addition, the system must have CJIS and FIPS 140-2 certification.

This includes backup media, file transfers and external sites. NYS shall be given all cryptographic keys used involving NYS data and systems.

13. Proposed system will be a multi-functional solution that combines a Records Management Database, a Training Management system, and a Learning Management System. The system must allow NYS staff to search the database and retrieve records by, but not be limited to, the following categories:
 - a. People: Searches all individual officer/employee records (See Appendix K.2, User Population)
 - b. Agencies: All employers of persons in the database (See Appendix K.2, User Population)
 - c. Learning Experiences: The 430 individual training courses that are approved by NYS (See Appendix K.5, Learning Experiences)
 - d. Events: The actual training courses (Learning Experiences) conducted by employers and reported to NYS
14. The existing application system uses an Oracle database to maintain all course, student, organizational and course history data. There are a total of 20 Oracle tables that contain data needed in the new system. It is expected that this existing data will be migrated and converted to the new database as provided by the chosen vendor. It is expected that this will include a commitment by existing State staff to provide assistance in data mapping and data quality review to ensure an accurate and complete conversion. Materials provided as part of this data conversion review will include a data dictionary and an entity-relationship diagram that will provide a primary description of how the existing data from the existing system is being stored as starting point for a detailed conversion specification to be developed by the selected vendor.
15. The proposed solution shall support the following internet browsers:
 - a. Microsoft Internet Explorer, versions 9 and 10 and any version released after 01-January-2014.
 - b. Apple Safari, versions 4, 5, 6 and 7 and any version released after 01-January-2014.
 - c. Firefox, versions 10 through 25 and any version released after 01-January-2014.
 - d. Google Chrome, versions 2 through 31 and any version released after 01-January-2014.

16. The Offerer's PSCTS design shall include, at a minimum:

- a. Hardware specification that is consistent with ITS portfolio of below listed supported platforms also listed in Appendix P.
 - a. Proposed Operating System shall be one of the following:
 - i. IBM POWER AIX
 - ii. Red Hat Enterprise Linux
 - iii. Microsoft Windows Server
 - b. Proposed Database (RDBMS) shall be one of the following:
 - i. Oracle
 - ii. MS SQL
 - iii. DB2
 - c. Proposed Web Servers shall be one of the following:
 - i. Apache
 - ii. Microsoft IIS
 - iii. IBM HTTP
 - iv. RedHat HTTP
 - d. Proposed Application Servers shall be one of the following:
 - i. J2EE
 - ii. WebSphere Application Server
 - iii. JBOSS
 - iv. Oracle WebLogic
 - v. .NET - - Microsoft IIS
 - e. Proposed Solution shall operate with the NYS ITS Authentication and Authorization Services
 - i. This service is based on LDAP and supports SAML and Netegrity SiteMinder to access the NYS Statewide Directory.
 - f. If Mainframe Services are proposed, the solution must be supported by either z/OS or z/Linux
 - g. Proposed solution shall be able to run effectively within a virtual server environment running on an approved operating system (see above).
- b. Software for all workflow, processing, and interface messaging to DCJS, DOS, DOH, NYSP, DHSES and NYS external partners (customers);
- c. Files and database requirements;
- d. Data storage requirements;
- e. Software
- f. Algorithms for searching and processing;
- g. Interoperability for internal and external partners, now and in the future.

17. The proposed solution will, to the maximum extent possible, automate all business processes listed in Appendix K Table 3

18. The proposed solution must keep to a minimum processes which require the exchange of paper or dependency on the vendor (e.g. reports).
19. User interface and data input must be user friendly to the average, non-technical individual and capable of self service at the Employer level. Requirements include:
 - a. Bulk upload features with real-time feedback to user for data correction.
 - b. User specific drop down fields
 - c. Automated calendaring
 - d. All opportunities to limit or eliminate manual typing (thus limiting opportunities for typographical errors)
20. System must provide the ability to allow the provider of training to review records of classes they or their agency/firm provided.
21. System must allow local agency training coordinators to access all training records of agency staff regardless of the provider of that training.
22. System must reduce the number of clicks required to submit or enter data. Pages containing information required for specified processes must have all details on one page. One example is the Annual Police Officer Registry update process which should have all required information contained in one page or screen, thus reducing time spent and opportunities for error created by navigating to various places in the application. A second example is completing training course information such as curriculum content forms and class rosters.
23. NYS requires a solution that allows secure and customizable access to eleven (11) levels of users. NYS also requires a solution that is capable of supporting users that may perform multiple roles for an employer and/or work for multiple employers. A description of the required levels of users is in Appendix K.4, User Access Levels. The system must:
 - a. provide access to all users listed in Appendix K.4
 - b. provide capability to support users that may have multiple roles for their employer . For example, a police officer may be employed full-time by a police department and require level 1 access, as described in Appendix K.4. This person may also serve as the training officer (level 2 access) for that department. This officer would need access commensurate with the job that could include the ability to update records of employees assigned to the department.

- c. Provide capability to support users that work for multiple employers. For example, an user may be employed a police officer and require level 1 access and be employed part -time as a security guard with another employer and would require level 6 access. Describe anticipated problems or concerns, if any, with records management.
 - d. Provide capability to manage records access for individuals with no affiliation to law enforcement. One example is the civilian security guard trainees that are not sworn officers or peace officers. Training is a pre-cursor to employment as a security guard and access to individual records by persons that have not been trained and/or certified is a concern.
 - e. Provide security solutions to support secure access to all users described in Appendix K.4
24. Interface with other State systems to provide for the exchange of data for example NYS Department of State (DOS), Department of Health (DOH), State Police (SP) and Division of Homeland Security and Emergency Services (DHSES). Ideally, these interfaces should provide the ability to interact as a web service between NYS and partner agencies. See Appendix K Table 4, User Access levels for more information.
25. Proposed system will assign each personnel record and each user agency or employer a unique identifier to be used as a customer account number when accessing the system.
26. Proposed solution will maintain a history for all training courses recognized by NYS. Currently, NYS recognizes 430 training courses and maintains data for every occurrence of the 430 courses. The proposed solution must allow NYS to continue to capture historical course data that includes; location, attendees, instructor(s), curricula, length of instruction in hours, and the NYS staff actions taken to review and approve each course. NYS's current Ingenium interface labels training courses as "Learning Experiences." The 430 Learning Experiences (Training Courses) are listed in Appendix K, Table 5.
27. The proposed solution must be capable of expansion to accommodate the addition of new Learning Experiences and new categories of police and peace officers. Refer to Appendix K, Table 5 for a listing of the current Learning Experiences and Appendix K, Table 9, CPL Definitions for Peace Officers and Appendix K, Table 10, CPL Definitions for Police Officer.

28. Proposed system allows for recording employment history of officers who have multiple job titles and the capacity in which they serve each employer. Additionally, the proposed system should be capable of maintaining a rank history throughout the officer's career.
29. The proposed solution will contain a Police and Peace Officer Registry database that is integrated and linked to the training provided by employers, academies and NYS. The proposed solution shall provide self-service for police and peace officers to gain access to their training record.
30. Proposed solution will contain a Security Guard Training Records Database that is integrated and linked to the training provided by employers, academies and NYS. The proposed solution shall provide self-service for security guards (civilians) to gain access to their training record.
31. Proposed System will allow employers of persons on the Police and Peace Officer Registry to self-service employee's records. Employers must be able to input, update, and validate details specific to each individual employed by them. In addition to the as needed records maintenance of assigned personnel, employers are required perform an Annual Validation of all their employees in the Police and Peace Officers Registry database. The specific details of the current processes for as needed or real-time registry changes are described on Appendix I.9, *Police and Peace Officer Registry Processes*. The current process for Annual Validation is described in Appendix I.10, *Annual Validation Process*.
32. Proposed solution will allow NYS to manage records relevant to law enforcement training courses administered by local training academies. This core business function is known as Course Approval. Refer to Curriculum Content Form and Class Roster documents within Appendix Q for data fields that NYS must capture during the course approval process. The specific details of the desired Course Approval and Completion Processes are depicted in flowcharts located in Appendix I.2 & I.3. The current processes for Course Approval, Course Completion, and Data Recording are depicted in Appendices I.4, I.5, and I.6, respectively. The system must:
 - a. Allow external providers to submit proposed courses and instructors for NYS pre-approval.
 - b. Allow NYS to review and approve the proposed training course and generate approval or disapproval notifications to the external provider.

- c. Enable external providers to submit rosters and course completion documents for approved courses to NYS for processing. Of importance is how the system allows data entry and interfaces with external systems rosters.
 - d. Allow NYS to audit the course rosters and documents for completeness and update individual records for trainees, instructors, employing agency and external providers.
 - e. Allow for the generation and distribution of course completion certificates, as required.
 - f. The proposed solution must include a process for NYS to process applications by new Security Guard Schools (NYS Approves Security Guard Training Schools). NYS must be able to receive, review and approve new applications as well as renewal applications. An automated solution to the process for school application and renewal is mandatory. The system must:
 - i. allow for the submission of initial security guard school applications
 - ii. Process submissions for two year recertification of schools
 - iii. Enable automated reminders for pending or expired school certifications
 - iv. Allow security guard employers to enter new employee records into the records system in a self-service model
 - v. distinguish between For-profit and Not-for-Profit Security Guard Schools to avoid charging fees to Not- for-Profit entities
 - vi. Provide for a self-service model of Data Entry of Rosters by employers, Academies, Security Guard Schools
33. The proposed solution will allow for the processing of data from Optical Mark Reader (OMR) bubble sheets submitted by Security Guard Program Employers. Employers submit course completion documentation from Security Guard Schools in the form of OMR (bubble sheets) that are scanned in. The current Security Guard Training process and details of the data submitted by OMR bubble sheets is depicted in a flowchart located in Appendix I.15. NYS envisions that the self service functionalities provided by the proposed solution will obviate the need for the aforementioned OMR process however the proposed solution must enable NYS to continue the OMR process for an indeterminate period to allow for an acceptable cut-over period for external customers.
34. Proposed solution will provide a self-service model allowing Security Guard Instructors to submit initial applications as well as recertification applications every five years.

35. Proposed solution will enable the training history of an officer, from recruit to retirement, to be recorded and accessible. The training history of each individual must follow all individuals regardless of change in Employer(s), or name(s). These histories must be accessible to authorized persons requiring access to this information such as record holder(s), employers, and NYS. The ability to meet the Agency Requirement is non-negotiable, the solution of how this requirement is met, is negotiable.
36. Proposed solution will allow for the administration of training course material for traditional in-residence classroom instruction provided by NYS staff, contract instructors, academies, and employers.
37. Proposed solution shall include a training course calendar and registration processes that:
 - a. allows NYS to assign or customize pre-requisites for course enrollments.
 - b. limits users ability to enroll in courses based on pre-requisites
 - c. allows self-registration by users.
 - d. generates customized registration approval or disapproval notices based on pre-requisites.
 - e. issues certificates upon course completion, and
 - f. performs records management updates upon course completion. Refer to Appendix K, Table 5, Learning Experiences, for a listing of current training courses and corresponding course pre-requisites.
38. The proposed solution shall include a means to produce configurable reports, as described in Appendix K Table 1, *Report Requirements*. Also, this solution will allow for NYS' ad hoc reporting.
39. NYS requires a solution that will identify gaps in the validity and expiration of training certificates and identify gaps in an officer's service from one employer to another. When a Peace or Police officer leaves employment his or her Basic Course for Police Officer (BCPO) certificate will remain valid for various time periods established by law. The periods of certificate validity depend on the length of the officer's prior continuous employment. For example; if an officer completes BCPO training and serves less than two (2) years before leaving employment, the officer has two years to become reemployed or the certificate is deemed invalid and requires the officer to complete additional "refresher" training. Likewise, an officer that serves more than two (2) consecutive years would have four (4) years before his or her BCPO certificate will become invalid. Finally, an officer has ten (10) years from the last date employment to complete a refresher course or the BCPO certificate is expired. In this case, the officer would need to repeat the entire BCPO course. NYS requires a registry

system that will identify and track gaps in training certificates such as the BCPO course as well as numerous other certifications that have expiration dates. The system must be capable of notifying NYS, employers and individual officers of existing gaps or the pending expirations of certifications. The system must contain a mechanism for NYS staff to provide final approval for any changes made by employers to resolve expired certificates. The system must allow NYS to assign maturity, validity and/or expiration dates to certain certificates or qualifications, make automated notifications, as appropriate to NYS staff, employers, and individual officers for expiring or expired certificates and allow NYS staff to provide final approval for any changes made by employers to resolve expired certificates. System shall allow for audits of training certificates and actions of system users

40. In order to manage compliance with training standards, NYS must be able to record, maintain and report on each officer's rank history, including transitions from one employer to another or from multiple employers and roles. This requirement coincides with the capability to provide gap analysis for validity of training certifications.
41. Proposed system will have a method to suppress and secure records of undercover officers and other individuals with similar requirements. Minimal, if any, workarounds are anticipated, processes must not be onerous.
42. Proposed solution shall deliver Reports in standard formats to include Adobe PDF and Microsoft Excel.
43. Proposed solution shall provide a reminder function to NYS Administrators and employers for due or overdue reports.
44. Proposed solution shall provide access by other state entities to verify and/or extract data. These users are identified in Appendix K Table 2 Population and their expected access is identified in Appendix K Table 4. User Level Access.
45. Proposed solution provides capability to produce standard and adhoc reports on specific courses to include;
 - a. geographic location held
 - b. course providers/instructors
 - c. Date and time course was held
 - d. number of courses held in a specific region

- 46. Proposed solution has ability to provide reports on student evaluations of training courses.
- 47. Proposed solution is capable of storing sample lesson plans, model training policies/memorandums and forms in Microsoft Word and PDF formats that can be downloaded by customers.
 - a. System must possess capability to accommodate MS Word/Excel/PowerPoint and Adobe@ PDF documents.
 - b. System must possess capability to accommodate documents (files) upwards of 4 GB in size.
 - c. System must possess capability of NYS Staff to upload/store documents in the system.
 - d. System must possess capability of customers to download documents.
- 48. Proposed solution must include documentation describing system functionality including Use Cases and requirements

Requisite Plans and Activities

- 49. Any proposals for changes made to PSCTS after system acceptance shall have prerequisite test and/or performance test results. This shall include upgrades, bug fixes, or changes that replace human intervention with any type of automated processing. The test plan and methodology for these proposals shall be approved by NYS.
- 50. As an initial deliverable after contract approval, the Contractor shall provide a Deliverables Acceptance Plan, for NYS approval, that will document formal procedures allowing each organization to fully understand their role and responsibility for deliverable acceptance, within a mutually agreed upon timeframe after contract approval.
 - a. Acceptance Testing Plan(s) must address
 - i. application,
 - ii. quality assurance processes,
 - iii. performance, and
 - iv. accuracy.
 - b. Acceptance Testing Plan(s) must articulate expected results and validation techniques for
 - i. accuracy

- ii. throughput
- iii. functionality, and
- iv. interoperability

51. “Acceptance” shall be defined as New York State written approval signifying that a deliverable meets expectations. A sample deliverable acceptance form is included in Appendix R Deliverables Acceptance Form. Verbal acceptance or acceptance by default is not sufficient. In order for a deliverable to be considered “complete” and “acceptable,” it must be measured against NYS acceptance criteria. To ensure timely acceptance of deliverables, the document must suggest the format, content and appearance of deliverables before they are produced. Items that must be defined are:
- a. The number and identity of stakeholders who may be required to review deliverables before final approval from the designated individual(s) is sought.
 - b. The number of business days in which deliverables must be either approved or rejected by the Customer.
 - c. Rework of portions of the deliverable, if required.
 - d. Resubmission of the deliverable.
 - e. The number of times a deliverable can be resubmitted to the Customer for approval.
 - f. The escalation process that will be followed if a timely decision on approval or rejection of a deliverable is not met.
52. The Contractor shall provide a Configuration Management Plan that describes its approach, tools and procedures to identify, baseline, track, audit and approve changes to the various components (software, documentation deliverables), within a mutually agreed upon timeframe after contract approval for NYS approval.
53. The Contractor shall provide a Testing and Acceptance Plan which provides that on-site testing and acceptance shall be performed by NYS in conjunction with the Contractor on all components, systems and subsystems, within a mutually agreed upon timeframe after contract approval. The Plan must include, but not be limited to, the acceptance testing elements specified in Appendix L and Appendix M. The plan shall provide that reports shall be produced by the Contractor and used by NYS to verify required functionality, throughput and accuracy, within a mutually agreed upon timeframe after contract approval for NYS approval.

54. The Contractor shall provide an Issue Management and Escalation Plan that will identify the critical steps of capturing, reporting, tracking and resolving issues in a timely manner and complies with the provisions of Section 5, within a mutually agreed upon timeframe after contract approval for NYS approval. At a minimum, this plan must identify:
- a. How issues will be captured and tracked
 - b. Ownership of each issue with expected resolution dates
 - c. Prioritization of issues allowing for triage
 - d. Fully developed escalation path for both the Contractor and NYS stakeholders
 - e. Process for plan refinement
55. The Contractor shall provide NYS Staff (System Administrators and IT Technical Support) with training, a Training Plan and training content that include, but are not limited to, all of the Training Plan Requirements specified in Appendix S, within a mutually agreed upon timeframe after contract approval for NYS approval.
56. NYS must have the ability to respond quickly and efficiently to all reporting requests, this includes requests for standard and ad-hoc information, without assistance from the vendor or need for advanced technical skill-set(s). The proposed system must allow NYS to create all standard reports, as described in Appendix K, Table 1 Report Requirement. NYS requires the ability create ad-hoc reports on any single field or multiple fields including but not limited to all items listed in Appendix K, Table 1. The system must generate standard and ad-hoc statistics on any single field or multiple fields including but not limited to all items listed in Appendix K, Table 1. NYS requires the ability to obtain report information without assistance from the vendor or need for advanced technical skill-set(s). The system must track and display month-to-month and year-to-year statistics for NYS staff work output that includes but is not limited to; number of training courses approved, training courses completed, individual records updated, persons trained, certificates issued, pistol permit verifications completed by the appropriate user access group, freedom of information requests, ad-hoc executive requests for reports, employer requests for records updates, individual requests for updates or transcripts, instructors certified and number of registry transactions.
57. The Contractor shall produce Production Reports which include, but are not limited to, the Production Report Requirements specified in Appendix K.1 within a mutually agreed upon timeframe after contract approval for NYS approval.

58. The Contractor shall provide a comprehensive Communications Plan that describes the means by which project communications will occur, within a mutually agreed upon timeframe after contract approval, for NYS approval. This Plan must emphasize the methods and tools by which bi-directional communication will be managed and executed. All project stakeholders must have a role within the Plan, and therefore the plan must fully define the expectations of both content and frequency. The plan must address:
- a. How often and how quickly information needs to be disseminated;
 - b. By what tools (example: e-mail) will information be exchanged;
 - c. What format the information will follow;
 - d. Roles and responsibilities of each participant

D. Optional Requirements-Separately Priced

System shall provide all capabilities required for NYS to stand-up an online or portal equivalent learning management system. System shall allow NYS to develop, manage and administer distance learning course offerings allowing for up to 1,500 concurrent users.

E. Project Plan

As part of the Technical Proposal, each Offerer must deliver a comprehensive Project Plan that clearly articulates a roadmap for success in implementing their solution. Offerers should refer to the NYS Guidebook for Project Management (available on the New York State Office OITS website at www.its.ny.gov/pmmp/guidebook2/index.htm) in formulating their response.

The purpose of the Project Plan response is to allow each Offerer to clearly articulate their methodology(s) and processes for the delivery and deployment of the proposed PSCTS (including software and any hardware components), as well as proposed timeframes, staffing requirements and other management proposals, e.g., risk management, quality management.

Each Offerer's proposed Project Plan must include the following elements:

1. Project Scope Description

Each Offerer must submit a Project Scope Description narrative which defines all work to be performed by the Offerer and all work to be performed by NYS or OITS to meet the project deliverables and requirements of the PSCTS as stated within the content of this RFP.

2. Project Schedule

The Offerer must submit as part of its proposal a comprehensive Project Schedule that includes a detailed list of the tasks, and the resources (e.g., Offerer and NYS), timeframes, deliverables and dependencies for each task.

One of the purposes of this RFP is to procure a PSCTS to replace the legacy systems currently in operation at NYS. The legacy NYS Public Safety Credentialing and Training System has exceeded the end of its useful life. The system operates on a 24x7x365 basis and presents maintenance issues. NYS establishes that the replacement of this system is the critical path for this procurement.

NYS requires that the replacement of the Public Safety Credentialing and Training System must be completed no later than September 1, 2015, and the Project Plans must reflect how the Offerer will accomplish this requirement including acceptance testing within the specified time period.

“Completed” means the following:

- The database conversions for the legacy data has been accomplished and the software has been delivered, installed and accepted as the production system; and
- Administrative on-site training for NYS staff has been provided; and
- Acceptance testing has been successful, and proven that all base requirements have been met; and
- The production system has been implemented and all Public Safety Credentialing and Training System processing has been transitioned to the COTS solution.

All critical milestones, deliverables, tasks, timeframes, dependencies and the schedules’ critical path must be clearly delineated within the Project Schedule and the defined milestones and delivery dates must directly relate to the Offerer supplied payment schedule in the cost proposal.

The Project Schedule must be fully resourced – all technical and functional roles (Offerer and NYS) required to meet the deliverables must be clearly identified.

The Project Schedule shall include, but not be limited to:

- a. the conversion of data;
- b. the acceptance of all software components;
- c. the acceptance by NYS of the successful results of all technical requirements testing;
- d. administrative staff on-site training
- e. the preparation of all components of the Production environment; and

- f. any Offerer customization of COTS software

Each Offerer must provide a comprehensive Project Schedule on a PC Compatible Windows Readable CD-ROM in adobe Acrobat® pdf format The Project Schedule must identify the items mentioned previously for all phases of the project. The plan must also include a Project view which clearly depicts a) critical path and b) major deliverables.

3. Narrative Description of Project Plan

Each Offerer must provide a narrative description of the Project Plan for implementation that includes a narrative description of the tasks, resources, timeframes, deliverables and dependencies for the delivery and deployment of the proposed Public Safety Credentialing and Training System (including software and hardware components).

One of the deliverables that must be included in the Project Plan is a transition plan for the current system and its interfaces, and databases from the current production system to the new Public Safety Credentialing and Training System The Offerer must provide a narrative description of the transition process that includes the tasks, resources, timeframes, deliverables, projected system unavailability time frames and dependencies for the transition. The narrative description should outline the specific procedures to be utilized to meet each deliverable for the transition. The narrative must allow NYS to completely interpret the procedures and their correlation to the tasks defined within the Project Schedule.

4. Staffing Management Plan

Each Offerer must submit a Staffing Management Plan that includes the following elements:

- a. The roles and responsibilities of both the Offerer and NYS organization for all phases of the project must be clearly delineated.
- b. The Offerer must submit the names of the Project Management Team (e.g., Project Manager, Testing Manager) to represent the Offerer and work directly with the NYS designated representative. The full resumes of the Project Management Team must be submitted with the Offerer response. In addition:
 - i. The Project Manager submitted by the Offerer shall have experience within the last five (5) years managing projects involving replacement of older Public Safety Credentialing and Training System with at least 30,000 training records with a new Public Safety Credentialing and

Training System using COTS products and services, and if necessary, customized products and services.

- ii. Following approval of the Contract. The Project Manager submitted by the Offerer shall be the Offerer's legal agent and NYS' prime contact with regard to all provisions of the Contract. The Project Manager must be made available to the NYS project at inception (full time) and remain with the project through the Warranty period. If for any reason the Project Manager is replaced, the replacement must have equal or higher qualifications than the original Project Manager and must be approved by NYS prior to any Project Manager staffing change.
- c. Staff requirements for both Offerer staff and corresponding NYS staff requested must be identified, including category of skill, skill set expectation, number of people by skill set and number of hours for each skill. The Offerers must clearly articulate the number and type of staff for the entire project and differentiate the roster between their implementation team and their post-implementation support/maintenance team.
 - i. An individual may appear on both rosters.
 - ii. The staffing plan presented in this section must correspond to the resources outlined in the Project Schedule presented in the Project Plan.
 - iii. A process must be described in the plan defining the Offerer responsibilities should NYS decide to remove a Vendor staff person from the project. This must include expected steps for requesting removal, backfill of a position and overlap for cross training, and NYS approval of the process. The narrative must be broad enough to cover both implementation and support personnel.
 - iv. The Offerer shall propose how it will work together with NYS during the contract term to minimize risks and schedule adjustments.
- d. The Offerer will maintain sole responsibility to NYS for work products produced by any subcontractor.
- e. If applicable, the Offerer shall describe their approach to problem resolution with any Subcontractor during contract execution.

5. Risk Management Plan

Mission critical projects demand management of risk, and a plan for mitigating actions to be deployed to manage risk before it impacts the project schedule or project success.

Each Offerer is required to submit a Risk Management Plan. The Plan shall clearly articulate the methods to be utilized in the identification of potential risks; the procedures utilized to predict the likelihood that a risk will occur; the methods for quantifying the potential impact to the project; and, the methods for development of action plans to mitigate the impact of that risk occurrence. The Offerer shall include information regarding best practices and, if applicable, lessons learned during the implementation of other complex PSCTS solutions that have been incorporated into the proposed Risk Management Plan. The risk management plan shall include:

- a. Proposed methods for identifying, analyzing and prioritizing risks; assessments of risk probability and impact; developing mitigation and contingency plans; documenting and tracking the status of risks; and monitoring ongoing actions to assess, monitor and mitigate risks throughout the project included in the plan;
- b. Plan includes a description of the roles, responsibilities, and training of those who participate in risk management activities and the types of risk tracking and monitoring records that will be maintained throughout the project; Plan includes when and how often the risk management process will be performed throughout the project and a designation of a risk owner.

NYS reserves the right to negotiate the Offerer proposed Risk Management plan should NYS find unacceptable the plan as proposed.

6. Quality Management Plan

The Offerer shall provide a Quality Management Plan that describes the processes and techniques to measure, monitor and control, the quality of the end product to ensure that PSCTS solution meets the objectives and provides the critical system features listed throughout this RFP.

The Offerer shall include information regarding best practices and lessons learned during the implementation of other complex PSCTS solutions that have been incorporated into the proposed Quality Management Plan. The quality management plan shall:

- a. Define and describe the processes and techniques to measure, monitor and control, the quality of the end product;
- b. Address both quality assurance and quality control requirements;
- c. Includes planning, developing, and implementing a quality management plan that can be implemented and supported (process audits, product assessments, corrective actions, and customer interface);
- d. Identifies the project's quality objectives and describe the tools, techniques, and methodologies for auditing, reviewing, testing, and evaluating deliverables, processes and services to determine conformance with the approved specifications at relevant stages of deliverable production

NYS reserves the right to negotiate the Offerer proposed Quality Management plan should NYS find unacceptable the plan as proposed.

7. Knowledge Transfer Plan

The Offerer shall provide a Knowledge Transfer plan that covers all aspects of the use, administration and technical support for the proposed solution.

NYS reserves the right to negotiate the Offerer proposed Knowledge Transfer plan should NYS find unacceptable the plan as proposed.

8. Conversion Plan

The Offerer shall provide a Conversion Plan that meets or exceeds NYS' needs and expectations as described in the Conversion Plan Requirements in Appendix L of this RFP.

NYS reserves the right to negotiate the Offerer proposed Conversion plan should NYS find unacceptable the plan as proposed.

3.2 Cost Specifications

As part of the Financial/Administrative Proposal, the Offerer is required to complete the cost response forms provided in Attachment 23 through Attachment 29. All costs provided in the attachments shall be in United States Dollars (\$ USD) and guaranteed throughout the term of the contract.

All pricing, fees and charges and not-to-exceed maximum rates to be paid by or on behalf of the State (“pricing”) submitted in Offerer’s proposal shall be held constant from the date the proposal is submitted to NYS, through the date on which the contract is approved by the Office of the State Comptroller and through the date on which NYS notifies the Contractor of its final acceptance of the conversion and of the system.

The pricing in effect as of the first day of the third year of the contract shall be established as the Contractor’s Base Year Pricing.

Each subsequent year thereafter for the duration of the contract and any renewal option exercised by the State, the Contractor shall be entitled to either hold or modify Contractor’s Pricing then in effect.

In the event that the Contractor elects to modify the Contractor’s Pricing, the Pricing then in effect shall be subject to either a maximum increase of the lesser of five percent (5%) or the percent increase in the National Consumer Price Index for All Urban Consumers (CPI-U) as published sixty (60) days prior to price increase request in the United States Bureau of Labor Statistics. In the event that the National Consumer Price Index for All Urban Consumers (CPI-U) is no longer available, another similar substitute Index acceptable to the Commissioner of the Office of General Services of the State of New York shall be used in its place.

The Offerer cost response will contain the following elements:

A. Proposed Fixed Purchase Price – Mandatory Base System - Attachment 23

The Offerer shall propose a fixed purchase price for the system as defined in its proposal for the mandatory base system. This price shall include all costs for software license fees, services, including knowledge transfer services, and any other type of deliverable or fee included in the fixed price.

B. Maintenance and Support Price – Mandatory Base System - Attachment 24

The Offerer shall propose a fixed-price maintenance and support schedule for the duration of the initial ten (10) year contract. The price shall include the retention of all Production and Test system software throughout the duration of the ten (10) year contract. This price must also include any costs that would be associated with converting NYS data to ensure operability with each upgrade. The Offerer shall provide a warranty period of one year from the date of system acceptance for all products and deliverables. This warranty period shall include full maintenance services at no additional cost to NYS. The Offerer solution shall include details of the proposed warranty to meet NYS’ needs as described in this RFP.

A key component of this project is to ensure that the technology platform(s) bid by each Offerer utilizes current and fully supportable release / version of Production and Test system software during implementation.

C. Optional Licensing and Professional Services Price List – Attachment 25

The Offerer shall provide a detailed Optional Licensing and Professional Services Price List that NYS, at its sole discretion, may choose to purchase throughout the duration of the contract. Include all possible models for licensing, including per user and enterprise models, and include all possible titles of staff (e.g., developers and engineers) in the list.

D. Total Proposed Cost for Offerer's Mandatory Base System for Initial 10 Year Contract Period – Attachment 26

The Offerer shall provide a total proposed Cost utilizing the format as defined in Attachment 26. This form summarizes the Total Cost which will be used for evaluation scoring purposes.

Note: For evaluation scoring purposes only, DCJS will assume we opt to purchase 1,000 additional licenses and 1,000 additional hours of professional services.

E. Proposed Fixed-Price Milestone Deliverable Payment Schedule – Attachment 27

The Offerer shall propose a fixed price milestone deliverable payment schedule. The overall payment schedule for the Proposed Fixed Purchase Price (Attachment 23, line d) will conform to the following principles:

1. Up to twenty five (25) percent of the fixed purchase price shall be payable to the Contractor upon acceptance of clearly defined and measureable deliverables to NYS prior to system implementation (see Glossary - Appendix N).
2. Fifty (50) percent of the fixed purchase price shall be held back by NYS and would not be payable to the Contractor until System Implementation.
3. The remaining twenty five (25) percent of the fixed purchase price shall be held back by NYS and would not be payable to the Contractor until all system defects have been repaired to the satisfaction of NYS and, in no event, would be payable to the Contractor prior to 180 calendar days following system implementation.

As a subset of the overall Proposed Fixed Purchase Price, a list of the Offerers' deliverables (as described in its Project Plan) associated payment schedule, and acceptance criteria shall be proposed by the Offerer. Pursuant to the payment terms described above, the Offerer shall propose a Fixed-Price Milestone Deliverable

Payment Schedule that shall total no more than twenty five (25) percent of the Proposed Fixed-Purchase Price as computed by the Offerer in Attachment 23, line d.

NYS will only make payment upon the signed acceptance of each deliverable by an authorized NYS representative. The deliverable and associated payment schedule submitted by each Offerer shall match the submitted Project Plan in their Microsoft Project work breakdown structure (WBS). There shall be a direct correlation between the deliverables submitted in the Project Plan and this deliverable payment schedule. NYS reserves the right to negotiate the Offerer requested payment schedule should NYS find unacceptable the schedule as proposed.

F. Detailed Optional Features Price List – Attachment 28

The Offerer shall indicate COTS, No Proposal or provide cost details for customization for each optional feature as detailed in RFP Section 3.1.D. The purchase of any optional feature is at the sole discretion of NYS. Do NOT include cost details if the optional feature is included in COTS or is not available.

G. Optional Services Price List – Attachment 29

Provide pricing for optional services that would be available to NYS at its discretion. Include services such as conversion and training (hourly or perhaps other scenarios such as per class). Examples include, but would not be limited to, additional conversion of electronic or paper records and training.

3.3 Administrative Specifications

The Offerer shall submit the documents identified in this section, properly completed, signed and notarized, if applicable, as part of the Financial/Administrative Proposal.

A. Firm Offer Letter and Conflict of Interest Disclosure

Each Offerer must submit an Offerer Firm Information Form (Attachment 5) and a formal offer in the form of a Formal Offer Letter as set forth in Attachment 11. The formal offer must be signed and executed by an individual with the capacity and legal authority to bind the Offerer in its offer to the State. The Offerer must accept all of the terms and conditions set forth in this RFP, including all amendments, appendices and attachments, and must agree to enter a contractual agreement containing, at a minimum, the terms and conditions identified in this RFP.

The Formal Offer Letter must include a statement affirming that the Bid Proposal is firm and binding for a period of at least one (1) year from the Bid Proposal Due date, or until such time as a Contract resulting from this RFP is approved by the NYS Comptroller. An Offerer's Bid Proposal may be withdrawn from consideration by the Offerer on written notice to DCJS if a Contract has not been approved by the NYS Comptroller after one (1) year following the submission of the Bid Proposal to DCJS.

The Formal Offer Letter must include a statement affirming that the proposed PSCTS solution meets or exceeds the mandatory base system requirements set forth in Subsection 3.1.C, including referenced attachments.

Each Offerer's Formal Offer Letter must include a Conflict of Interest Disclosure, in the form set forth in Attachment 11, stating that the Offerer knows of no factors existing at time of bid submission or which are anticipated to arise thereafter, which would constitute a potential conflict of interest in successfully meeting the contractual obligations set forth herein, including but not limited to:

1. No potential for conflict of interest on the part of the Offerer due to prior, current or proposed contracts, engagements, or affiliations; and
2. No potential conflicts in the sequence or timing of the proposed award under this RFP relative to the timeframe for service delivery, or personnel or financial resource commitments of Offerer to other projects.

B. Contract Administration Team

The Offerer shall submit a Resolution of the Corporate Board of Directors, which names the individual(s) who can submit a proposal in response to this RFP and has the authority to act for the Offerer with respect to all administrative requirements of this procurement, including but not limited to, execution and processing of Contract documents, billing and fiscal inquiries, delivery of documentation and required reports should an award be made to the Offerer. The Resolution of the Corporate Board of Directors shall be submitted as part of the Offerer's Financial/Administrative Proposal, enclosed with Attachment 11.

C. Mandatory Requirement – MacBride Fair Employment Principles

The Offerer must agree to abide by the provisions of the MacBride Fair Employment Principles as outlined in Section 174-b of the State Finance Law (see Attachment 12). Compliance with said principles must be certified by completion of the Non-Discrimination in Employment in Northern Ireland Statement, Attachment 12, which shall be submitted as part of the Financial/Administrative Proposal.

D. Mandatory Requirement – Non-Collusive Bidding Certification

Each Offerer shall submit, as part of the Financial/Administrative Proposal, a completed copy of the Non-Collusive Bidding Certification, which is included as Attachment 13. This will certify that, to the best of the Offerer's knowledge and belief that:

1. The prices in the bid have been arrived at independently, without collusion, consultation, communication or agreement, for the purpose of restricting competition, as to any matter relating to such prices, with any other Offerer or with any competitor; and
2. Unless otherwise required by law, the prices which have been quoted in the bid have not been knowingly disclosed by the Offerer and will not knowingly be disclosed by the Offerer, directly or indirectly, to any other Offerer or to any competitor prior to completion of the selection process; and
3. No attempt has been made or will be made by the Offerer to induce any other person, partnership or corporation to submit or not to submit a bid for the purpose of restricting competition.

In accordance with NYS Finance Law Section 139-d, a bid shall not be considered for award nor shall any award be made where the above conditions have not been complied with; provided, however, that if in any case the Offerer cannot make the foregoing certification, the Offerer shall so state and shall furnish with the bid a signed statement which sets forth in detail the reasons therefore. Where the above conditions have not been complied with, the bid shall not be considered for award nor shall any award be made unless the Director of Finance and Administration of DCJS determines that such disclosure was not made for the purpose of restricting competition.

The fact that an Offerer has published price lists, rates, or tariffs covering items or services being procured, has informed prospective customers of proposed or pending publication of new or revised price lists for such items, or has sold the same items to other customers at the same prices being bid, does not constitute a disclosure within the meaning stated above.

E. Mandatory Requirement - Procurement Lobbying

Offerers are required to comply with the DCJS Procurement Lobbying Guidelines, Attachment 14. Offerers are required to complete and submit the following Attachment 14 forms as part of their Financial/Administrative Proposal:

Form 1 – Offerer’s Affirmation of Understanding of and Agreement Pursuant to State Finance Law § 139-j(3) and § 139-j (6) (b)

Form 2 - Offerer Disclosure of Prior Non-Responsibility Determinations

Form 3 – Offerer’s Certification of Compliance with State Finance Law § 139-k(5)

F. Mandatory Requirement - Provisions of NYS Tax Law §5-A

Section 5-a of the Tax Law of the State of New York, as amended effective April 26, 2006, requires certain contractors who have been awarded state contracts for commodities, services and technology valued at more than \$100,000 to certify to the State of New York Department of Taxation and Finance that they are registered to collect New York State and local sales and compensating use taxes. The law applies to contracts where the total amount of such contractors’ sales delivered into New York State are in excess of \$300,000 for the four quarterly periods immediately preceding the quarterly period in which the certification is made, and with respect to any affiliates and subcontractors whose sales delivered into New York State exceeded \$300,000 for the four quarterly periods immediately preceding the quarterly period in which the certification is made.

This law imposes upon certain contractors the obligation to certify whether or not the contractor, its affiliates, and its subcontractors are required to register to collect state sales and compensating use tax and contractors must certify to DTF that each affiliate and subcontractor exceeding such sales threshold is registered with DTF to collect New York State and local sales and compensating use taxes. The law prohibits the Office of the State Comptroller and other approving agencies, from approving a contract awarded to a contractor subject to the registration requirement but who is not so registered in accordance with the law.

Contractor certification forms and instructions for completing the forms are attached to this bid, Attachment 15. Form No. ST-220-TD must be filed with and returned directly to DTF. Unless the information upon which the ST-220-TD is based has changed, this form only need be filed once with DTF. If the information changes for the contractor, its affiliate(s), or its subcontractor(s), a new Form No. ST-220-TD must be filed with DTF. Form ST-220-CA must be filed with the Financial/Administrative Proposal and submitted to DCJS as the procuring covered agency certifying that the contractor filed the ST-220-TD with DTF. Failure to make either of these filings may render an Offerer non-responsive and non-responsible. Offerers shall take the necessary steps to provide properly certified forms within a timely manner to ensure compliance with the law.

Offerers may call DTF at **1-800-698-2909** for any and all questions relating to Section 5-a of the Tax Law and relating to a company's registration status with the DTF. For additional information visit DTF on the Internet at:

<http://www.tax.ny.gov/>

G. Mandatory Requirement – NYS Standard Vendor Responsibility Questionnaire

Offerer and all key subcontractors must fully and accurately complete the NYS Standard Vendor Responsibility Questionnaire, certifying to the requirements therein, which is attached as Attachment 16 (hereinafter the “Questionnaire”). Offerers are invited to file the Questionnaire online via the New York State VendRep System or they must complete and submit a paper Questionnaire (Attachment 16) as part of their Financial/Administrative Proposal. Offerers must also complete and submit the Vendor Responsibility affirmation provided on Attachment 11, Firm Offer Letter and Conflict of Interest Disclosure.

To enroll in and use the New York State VendRep System, see the VendRep System Instructions available at <http://www.osc.state.ny.us/vendrep> or go directly to the VendRep System online at http://www.osc.state.ny.us/vendrep/info_vrsystem_vendor.htm . For direct VendRep System user assistance, the OSC Help Desk may be reached at 866-370-4672 or 518-408-4672 or by e-mail at <mailto:ciohelpdesk@osc.state.ny.us> .

The Offerer acknowledges that the State’s execution of the Contract will be contingent upon the State’s determination that the Offerer is responsible, and that the State will be relying upon the Offerer’s responses to the Questionnaire in making that determination. The Offerer agrees that if it is later found by the State that the Offerer’s responses to the Questionnaire were intentionally false or intentionally incomplete, on such finding, DCJS may terminate the Contract by providing ten (10) days written notification to the Contractor, or declare the proposal non responsive. In no case shall such termination of the Contract by the State be deemed a breach thereof, nor shall the State be liable for any damages for lost profits or otherwise, which may be sustained by the Contractor as a result of such termination. Offerers are notified that evaluation of Vendor Responsibility may be separately made by or based on records of government agencies in addition to DCJS, including but not limited to the Office of the State Comptroller, the Office of the Attorney General and the NYS Department of Taxation and Finance and the Secretary of State.

H. Encouraging Use of NYS Businesses in Contract Performance

Each Offerer shall complete and submit the form entitled Encouraging Use of NYS Business in Contract Performance, Attachment 17, to indicate whether or not New York State Businesses will be used in the performance of this contract.

I. Proposed Subcontractors

Each Offerer shall submit a list of the subcontractors proposed for use on the PSCTS project on Attachment 18.

J. Key Subcontractor Certification

Each Offerer shall submit, for each key subcontractor (as defined in the Glossary – Appendix S) proposed by the Offerer, a Key Subcontractor Certification, Attachment 19, that has been completed and executed by the proposed key subcontractor's authorized representative. Each proposed key subcontractor must complete and execute a Key Subcontractor Certification form.

K. Consultant Disclosure

Consultant Disclosure - State Finance Law §163(4)(g) requires the selected Contractor to complete and submit an initial planned employment data report and an annual employment report regarding the number of persons employed to provide services under the contract, the number of hours worked and the amount paid to the Contractor by the State. It includes all employees providing services whether employed by the Contractor or a subcontractor. Form A – Contractor's Planned Employment From Contract Start Date Through The End Of The Contract Term Form B – Contractor's Annual Employment Report are attached for your reference. See Appendix E: Consultant Disclosure Forms.

Form A - Contractor's Planned Employment Form must be submitted as part of any winning Offerer's bid response before it can be submitted to the Office of the State Comptroller for approval. DCJS will coordinate with the winning Offerer to complete this form.

Each Offerer shall submit an Consultant Services Contractor's Annual Employment Report (Form B) Addendum Attachment 21, agreement to comply with the annual Form B reporting requirement pursuant to State Finance Law §163(4)(g). Each Offerer's Addendum, Attachment 21, must be properly completed, signed by the Contractor's authorized representative and notarized.

Form B - Contractor's Annual Employment Report. Offerer agrees to annually submit Form B each year that the contract is in effect and will detail employment data for the most recent concluded State fiscal year (April 1 – March 31). Instructions for these forms follow. Form B must be submitted by May 15th of each year to the NYS Division of Criminal Justice Services, the NYS Office of the State Comptroller and

the NYS Department of Civil Service. The first Form B must be submitted by May 15, 2015. The Offerer agrees to simultaneously report such information to the NYS Division of Criminal Justice Services, the NYS Office of the State Comptroller and the NYS Department of Civil Service as designated below:

State of New York Division of Criminal Justice Services
Office of Financial Services
Alfred E. Smith Office Building
80 South Swan Street, 10th Floor
Albany, New York 12210

NYS Office of the State Comptroller
Bureau of Contracts
Attn: Consultant Reporting
Bureau of Contracts
110 State Street, 11th Floor
Albany, NY 12236

NYS Department of Civil Service
Attn: Consultant Reporting
Empire State Plaza, Swan Street Building #1
Albany, NY 12239

L. Non-Disclosure Agreement

A non-disclosure agreement executed by the bidder and any known or identified subcontractor is required as part of the response to this RFP (see Attachment 2). Contractor and subcontractor staff may be required to complete a non-disclosure agreement at the time they are assigned to the project.

M. Staffing Plan

Consistent with the Equal Employment Opportunity Requirements of Section 5.31 of the RFP, Please prepare and submit a Staffing Plan, Attachment 9.

N. MWBE Utilization Plan

Please provide a MWBE utilization Plan, Attachment 10, including a detailed description of the supplies and/or services to be provided by each certified Minority and Women-owned Business Enterprise (M/WBE) under the contract.

4.0 Evaluation and Scoring Method

4.1 Overall Proposal Evaluation Process

New York State expects to award this project to one (1) Offerer.

Each Offerer must meet all the mandatory requirements. Offerers not meeting the mandatory qualifying experience requirements will be disqualified from further consideration.

Pursuant to Article XI of the State Finance Law, the basis for an award of this project is a best-value offer which optimizes quality, cost and efficiency, among responsive and responsible Offerers, and which is consistent with the best interest of New York State.

The State intends that all proposals will be evaluated uniformly and consistently, ensuring Offerers that each has an equal opportunity to be considered. The evaluation process will be conducted by a committee selected by the State.

Offerers may be requested to clarify contents of their proposals. No Offerer will be allowed to alter its proposal or add new information after the filing date. Minor omissions may be corrected at the discretion of the State. In addition to evaluating the material submitted by the Offerer in response to this RFP, NYS reserves the right to consider any and all additional sources of information and to use that information in determining its final bid selection.

Proposals submitted by Offerers will be first evaluated to determine whether all of the mandatory requirements identified in this RFP have been met. Proposals that do not meet all mandatory requirements will be deemed non-responsive and will not be further evaluated.

Offerers are hereby apprised of the relative importance or weight of the cost criterion compared with the overall non-cost criterion as follows, with the evaluation criteria being applied equally and uniformly in the evaluation of proposals:

The Technical Evaluation will account for 70% of the total evaluation scoring at 70 out of 100 total points, with the remaining 30% of the evaluation of 30 out of 100 total points based on the Cost Proposal.

4.2 Timeliness and Completeness Review

After the bid opening, each proposal will be screened for timeliness, completeness and conformance with the requirements as specified in Section 2.5 (Proposal Format and Content Requirements). Proposals that do not meet the requirements as set forth in this

RFP may be deemed non-responsive, removed from further consideration and the Offerer notified accordingly. Proposals that pass the Timeliness and Completeness Review will proceed to the Technical Mandatory Evaluation.

4.3 Mandatory Qualifying Experience - Technical Evaluation (Pass / Fail)

Proposals will be evaluated against the mandatory qualifying experience (Pass/Fail) Requirements described in Section 3.1.B and Section 3.1.C. Each Offerer must meet the Offerer mandatory qualifying experience and customer reference requirements specified in Section 3.1.B of the RFP, and each Offerer's proposed Public Safety Credentialing and Training solution must meet the mandatory base system requirements specified in Section 3.1.C of the RFP. As part of their Financial/Administrative Proposal, the Offerer shall submit a Firm Offer Letter, as set forth in Attachment 11, which shall include a statement affirming that the Offerer's proposed PSCTS solution meets or exceeds all of the mandatory base system requirements set forth in Section 3.1.C. Offerers not meeting those mandatory requirements will be disqualified from further evaluation and the Offerer will be notified accordingly. Offerers that are tentatively determined to meet mandatory qualifying experience requirements will proceed to the Technical Preferred and Financial Evaluations.

Verification Process

Technical evaluation staff will seek Customer Reference verification for all bids that tentatively meet the mandatory qualifying experience by contacting all customer references (maximum of 7) and requesting the reference to complete and respond by the due date (1 week) to the Customer Reference Questionnaire, Attachment F. Staff may follow up by phone as needed in an effort to secure the Customer Reference responses, and may extend the due date within reason to secure verification of the mandatory qualifying experience.

If NYS is unable to obtain the necessary minimum reference responses to verify the mandatory qualifying experience and mandatory requirements as specified in Section 3.1.B and Section 3.1.C of the RFP, the Offerer may be notified to allow the Offerer to encourage the references to respond. NYS reserves the right to contact customers for clarification of responses given in the questionnaire. If NYS is unable to verify the mandatory qualifying experience through customer references, the offer will be deemed non-responsive.

In the event an offerer submits more than 7 customer references, NYS will utilize the first 2 listed references as necessary to verify the mandatory qualifying experience, and will seek up to 7 customer references in the order listed in the bid response.

Proposals that do not satisfy the mandatory qualifying experience requirements will be removed from further consideration and the Offerer will be notified accordingly.

4.4 Preferred Technical Evaluation (70 Points)

The Preferred Technical Evaluation will be worth 70 points and will consist of an evaluation of the Offerer's Technical Proposal response. The Preferred Technical Evaluation will be conducted by the Technical Evaluation Teams, concurrent with and independent from the Financial Evaluation, which will be performed by the NYS Office of Financial Services, and concurrent with the Mandatory Qualifying Experience verification process discussed in Section 4.3.

Bid proposals will be scored as follows:

Customer Rereferences Experience with Vendor	6 Points
Executive Summary Evaluation	5 Points
Base System Requirements - COTS/Customize Attachment 7	20 Points
Base System Requirements - Solution Descriptions Attachment 8	28 Points
Conversion Plan	6 Points
Project Plan	5 Points
	70 Points

4.5 Financial (Cost) Evaluation (30 Points)

The Financial Evaluation will be worth 30 points and will consist of an evaluation of the Offerer's Financial/Administrative Proposal response to all of the elements described in Section 3.2 of the RFP and on Attachments 23-29. The Financial Evaluation will be a two (2) part evaluation as follows:

- 25 points will be based on total cost for Offerer's mandatory base system for the initial ten (10) year contract term (Attachment 26), including the fixed purchase price, the related maintenance and support cost, and, for evaluation scoring purposes only, the proposed cost to add 1,000 additional users and 1,000 hours worth of optional services based on the average hourly fee. The Offerer/Contractor shall provide a warranty period of one year from the date of system acceptance for all products and deliverables. This warranty period shall include full maintenance services at no additional cost to NYS.

The lowest cost Offerer receives 25 points, and all other Offerers are evaluated relative to the lowest Offerer's cost. The formula for the evaluation of other Offerers cost will be $(\text{Lowest Cost Offerer} / \text{Offerer Cost}) \times 25$.

- Five (5) points will be based on the Detailed Optional Features Price List (Attachment 28). The sum of the Total Optional Feature Cost and the Total Monthly Maintenance Cost will be used to determine the Offerer's Detailed Optional Features cost. The lowest cost Offerer receives five (5) points, and all other Offerers are evaluated relative to the lowest Offerer's cost. The formula for the evaluation of other Offerers cost will be $(\text{Lowest Cost Offerer} / \text{Offerer Cost}) \times 5$.

4.6 Final Proposal Ranking

Offerer's scores from the Technical Preferred Evaluation and the Financial Evaluation will be combined to produce a total score. The proposals will be ranked based on the total scores. The Offerer with the highest total score will be the winner of a tentative award subject to successful contract negotiations and Attorney General and Office of the State Comptroller approval.

In the event two proposals are found to be substantially equivalent, price shall be the basis for determining the award recipient or, when price and other factors are found to be substantially equivalent, the determination of the agency head or designee to award a contract to one or more of such Offerers shall be final.

The approved bid award(s) between the State and the successful Offerer will not be binding until it has been approved in accordance with New York State's contract approval process.

5.0 Other Terms and Conditions

In addition to contractual provisions set forth in Section 2 of this RFP, the following other terms and conditions shall apply:

5.1 Governing Law

The laws of the State of New York shall govern this procurement and the Contract and all subcontracts issued hereunder. Actions or proceedings arising there from shall be heard in a court of competent jurisdiction in the State of New York. The terms of Appendix A, *Standard Clauses for New York State Contracts*, are expressly incorporated in this solicitation and the Contract as though set forth in their entirety herein.

5.2 Substantial/Material Change

The provisions of the State Finance Law §138 mandate the State's approval of subcontractors. Throughout the Contract term, in the event that there is a substantial or material change in the ownership or financial viability of the Contractor, its corporate affiliates, subsidiaries or divisions, or that of any key subcontractors as defined herein, the Contractor is required to provide notice and details of any such change to NYS in writing immediately when such is first known by Contractor, its corporate affiliates, subsidiaries or divisions, or key subcontractors.

“Substantial” or “material” change shall be defined to include, but not be limited to, sale, acquisitions, mergers or takeovers involving the Contractor, its corporate affiliates, subsidiaries or divisions, or key subcontractors which result in a change in the controlling ownership or assets of such entity after the submission of the Bid Proposal; or entry of an order for relief under Title 11 of the United States Code; the making of a general assignment for the benefit of creditors; the appointment of a general receiver or trustee in bankruptcy of Contractor's, its corporate affiliates, subsidiaries or divisions, or key subcontractors and partners' business or property; or action by Contractor, its corporate affiliates, subsidiaries or divisions, or key subcontractors and partners under any state insolvency or similar law for the purposes of its bankruptcy, reorganization or liquidation; or court ordered liquidation against Contractor, its corporate affiliates, subsidiaries or divisions, or key subcontractors and partners.

Upon NYS' receipt of such notice, NYS shall have a minimum of thirty (30) business days from the date of notice to review the information. The Contractor may not transfer the Contract among corporate affiliates, subsidiaries or divisions without the advance written consent of NYS and the New York State Office of State Comptroller, where applicable. In addition to any other remedies available at law or equity, NYS shall have the right to prospectively cancel the Contract, in whole or in part for cause if it finds that such change materially and adversely affects the security, completion or ongoing

operation of the PSCTS, solely determined with reference to the best interests of NYS and the Authorized Users of the PSCTS.

5.3 Changes in Contractor's Project Team

Contractor will provide thirty (30) business days advance notice to NYS in the event of a proposed change in the Project Team, or any key subcontractors named in the Bid Proposal. Such changes must be approved in writing in advance by the State. Upon the State's receipt of such notice, the State shall have thirty (30) business days from the date of notice to review the information. In addition to any other remedies available at law or equity, the State shall have the right to prospectively cancel the Contract, in whole or in part for cause if it finds that such change materially and adversely affects the security, completion or ongoing operation of the PSCTS, solely determined with reference to the best interests of the State. During the Contract term, the State agrees that it will not unreasonably withhold its consent to subcontractors. If exigent circumstances are present, the State will give the Contractor written notice of such circumstances requiring extension and the Parties may thereafter extend the thirty (30) business days for an additional thirty (30) business days in order to complete its review.

5.4 Third Party Beneficiary Requirement

Unless waived by the State, all subcontracts between the Contractor and a key subcontractor shall expressly name the State of New York as an intended third party beneficiary of such contracts.

5.5 Qualified Project Personnel

Personnel providing services on this project must be licensed or certified professionals where required by law. The Contractor must certify that equipment and service technicians are trained and qualified for the work being performed by the manufacturer of the proposed equipment, database management or software application developers. In the event that the Contractor identifies personnel for assignment to this project to NYS in its proposal, the Contractor agrees not to reassign such identified personnel away from the project without the consent of NYS, which consent shall not be unreasonably withheld.

5.6 Quality of Service

Should it be found that the quality of services being performed by the Contractor under the Contract, in whole or in part, are not in compliance with the Contract service requirements, the State may declare Contractor in default in accordance with the *Termination* section below.

5.7 Ongoing Reports/Documentation

The Contractor shall provide project reports/documentation as a condition precedent to payment under the Contract. Failure to provide a report required within the due date may subject the Contractor to other actions determined appropriate by the State set forth herein. Upon notice, the Contractor shall have an opportunity to cure the default or be subject to Contract termination. The State's failure to demand or receive required documentation shall not be deemed a waiver of rights under this paragraph.

All reports shall be delivered electronically. The parties to the Contract shall agree to an electronic format (e.g., application and required data elements) for any reports. Each report shall be transmitted to NYS electronically via the internet utilizing encryption standards and protocols approved by the State, where applicable, and the system used shall generate an electronic ticket acknowledging transmission.

All weekly reports required under this section shall be due within two (2) business days after the last day of the required reporting period. All other reports which may be required under this RFP shall be due within ten (10) business days after the designated reporting period established by the State.

Design, Conversion and Build Reports

During the Design, Conversion and Build Phase, the Contractor will provide the State with weekly reports of all activities to date. Such reports to include, but not be limited to:

1. Database Design, Conversion progress, testing of proposed schema
2. Selection and reporting of subcontractors
3. Progress reports on test system production systems
4. System Testing Reports from Contractor testing
5. Acceptance Testing Results
6. Integration Plan including Plans for Transition/Cutover
7. Progress of All Work
8. Updated, As-Built Design Drawings

The Contractor shall hold a series of walkthroughs of its documentation for the State in advance of critical milestones. Materials to be reviewed at each walkthrough shall be delivered to the State at least two (2) weeks prior to the scheduled date of the walkthrough. Prior to System Implementation, the Contractor shall provide documentation about scalability, interoperability, performance and security of the proposed system for review by the State Architecture team. System Implementation shall not take place without approval of this material by the State Architecture team.

5.8 Insurance and Maintenance Bond

A. General

The Contractor shall file with the DCJS Office of Financial Services, Certificates of Insurance evidencing compliance with all requirements contained in this RFP no more than thirty (30) calendar days after receipt of "Notice of Contract Award" from the State and annually thereafter. Such Certificates of Insurance shall be of form and substance acceptable to the State. Acceptance and/or approval of NYS of the Certificates of Insurance does not and shall not be construed to relieve the Contractor of any obligations, responsibilities or liabilities under the Contract. All insurance required by the Contract shall be for the performance of the Contractor's obligations during the term of this Contract, and shall be obtained at the sole cost and expense of the Contractor, and shall be maintained with insurance carriers licensed or authorized by the New York State Department of Financial Services to issue insurance in the State of New York; In addition, all such insurance policies shall provide that the required coverage shall apply on a primary and not on an excess or contributing basis as to any other insurance that may be available to DCJS and/or the State of New York for any claim arising from the Contractor's work under this Contract, or as a result of the Contractor's activities. Any other insurance maintained by NYS or the State of New York shall be excess of and shall not contribute with the Contractor's insurance regardless of the "other insurance" clause contained in NYS or the State's own policy of insurance. Further, Contractor's insurance policies, unless otherwise mutually agreed by the State, shall be endorsed to provide that written notice must be given to NYS at least thirty (30) calendar days prior to cancellation, non-renewal, or material alteration of such policy or policies, which notice, evidenced by return receipt of United States Certified Mail shall be sent to the NYS Project Manager. The insurance policies shall name the State of New York, its Officers, agents and employees as additional insured's thereunder.

B. Payment of Premium & Deductible

The Contractor shall be solely responsible for the payment of all premiums and deductibles to which all such policies are subject, and the State shall have the right, in the event of a default or other failure by the Contractor to make a premium or deductible payment associated with the coverage's set forth in this section, to pay the required premium(s) or to settle the outstanding balance due with a carrier and to deduct the cost therefore from any sums otherwise due the Contractor under the agreement.

C. Carrier(s)

Insurance shall be maintained with insurance carriers licensed to do business in New York State. Each insurance carrier must be rated with an A.M. Best Company rating of "A-" Class "VII" or better in the most recently published Best's Insurance Report. If, during the term of the policy, a carrier's rating falls below "A-" Class "VII," the insurance must be replaced no later than thirty (30) calendar days from the date of the

negative rating change or the renewal date of the policy, whichever occurs sooner, with an insurer acceptable to the State and rated at least "A-" Class "VII" in the most recently published Best's Insurance Report.

D. Coverage Term

The Contractor shall cause all insurance to be in full force and effect as of the date that the Contract resulting from this RFP is approved by the Office of the State Comptroller and to remain in full force and effect throughout the term of the Contract and as otherwise required by the terms and conditions of the Contract. The Contractor shall not take any action, or omit to take any action, that would suspend or invalidate any of the required coverage's during the period of time such coverage's are required to be in effect. Not less than 30 calendar days prior to the expiration or renewal date the Contractor shall supply the State updated replacement Certificates of Insurance, and amendatory endorsements.

E. Form of Insurance

The required insurance certificates shall: (1) name the People of the State of New York, its officers and agents as additional insureds, (2) be in a form and substance acceptable to the State; (3) be obtained at the sole cost and expense of the Contractor; (4) be maintained with insurance carriers licensed or otherwise authorized to do business in New York who are acceptable to State; (5) be primary and non-contributing to any insurance or self-insurance maintained by the State; (6) contain the standard ISO separation-of-insureds provision, or a substantially similar clause; (7) be endorsed to provide written notice to the State at least 30 calendar days prior to the cancellation, non-renewal, or material alteration of such policies, which notice shall be evidenced by return receipt of United States Certified Mail sent to the attention of:

Procurement Officer
State of New York Division of Criminal Justice Services
Office of Financial Services
Alfred E. Smith Building
80 South Swan Street, 10th Floor
Albany, New York 12210

In no event shall any certificate form's cancellation provision, contain the words "endeavor to" and/or "but failure to mail such notice shall impose no obligation or liability of any kind upon the company, its agents, or representatives" or similar language within its provisions.

F. Subcontractor Insurance

Additionally, the Contractor shall require all of its subcontractors performing work in connection with the Contract, prior to commencement of an agreement between Contractor and the Subcontractor, to secure and keep in force during the term of their

contractual services, the applicable insurance requirements of this section. Satisfactory proof thereof shall be supplied by the Contractor to DCJS Procurement Officer or where applicable to such other State official or employee designated by the State upon request.

G. Right to Make Claim

The failure of: (1) the Contractor to furnish certificates that comply with the requirements of the Contract, or (2) the State to demand such certificate or other evidence of full compliance with these insurance requirements, or (3) the State to identify a deficiency from evidence that is provided to the State, or (4) the State to make payment on behalf of the Contractor in order to maintain required coverage's, shall not be construed as a waiver of the State right's to enforce the provisions of this section, or as a waiver of the Contractor's liability for failure to meet the insurance requirements set forth herein. In addition to any other legal or equitable remedies that may be available to the State, failure to maintain the required insurance may, in the State's sole judgment, be grounds for a termination of the Agreement for cause. By requiring insurance, the State does not represent that coverage and limits will necessarily be adequate to protect the State and such coverage and limits shall not be deemed as a limitation on the Contractor's liability to the State under the Contract.

H. Commercial General Liability & Umbrella Liability Insurance

The Contractor shall maintain commercial general liability (CGL) and, if necessary, commercial umbrella insurance with a limit of not less than two million dollars annually for each occurrence which shall be effective as of the date of approval of the contract by the New York State Comptroller. Such liability shall be written on ISO occurrence form CG 00 01 01 96(or a substitute form providing equivalent coverage) and shall cover applicable liability arising from premises, operations, independent contractors, subcontractors, all product (including any equipment and system components) completed operations during the contract period, broad form property damage, personal injury, defense and/or indemnifications obligations, including obligations under any resulting Contract, cross liability coverage and liability assumed in a contract (including the tort liability of another assumed in a contract). The State shall be included as an insured under the CGL, using ISO additional-insured endorsement (General Liability Additional-Insured Endorsement shall be on Insurance Service Office's (ISO's) form number CG 20 10 11 85) or a substitute providing equivalent coverage, and under the commercial umbrella, if any. This insurance shall apply as primary insurance with respect to any other insurance or self-insurance programs afforded to the State. The Contractor shall submit insurance verification information acceptable to the State upon request.

I. Comprehensive Professional Liability Insurance

If providing professional services, the Contractor shall maintain — or if subcontracting professional services, shall certify that Subcontractor maintains — errors and omissions liability insurance with a limit of not less than one million dollars per loss annually. Such

insurance shall apply to professional errors, acts, or omissions arising out of the scope of services covered by this Contract and may not exclude bodily injury, property damage, testing, monitoring, measuring, or laboratory analyses, where applicable. If coverage is written on a claims-made policy, the Contractor warrants that any applicable retroactive date precedes the effective date of this Contract; and that continuous coverage will be maintained throughout the contract.

J. Liability Insurance Policies/State Designation

Any aforementioned Insurance Policies issued must be in the name of “The People of the State of New York”, with appropriate dollar coverage.

K. New York State Worker’s Compensation Law

Sections 57 and 220 of the New York State Workers’ Compensation Law (WCL) provide that the State shall not enter into any contract unless proof of workers’ compensation and disability benefits insurance coverage is produced. Prior to entering into a contract with the State, any successful Contractor will be required to verify for the State, on forms authorized by the New York State Workers’ Compensation Board, the fact that they are properly insured or are otherwise in compliance with the insurance provisions of the WCL. The forms to be used to show compliance with the WCL are listed below. The State would prefer submission of insurance verification information with interested bids. Any questions relating to either workers’ compensation or disability benefits coverage should be directed to the State of New York Workers’ Compensation Board, Bureau of Compliance at 1-866-298-7830. Failure to provide verification of either of these types of insurance coverage by the time winning bids have been selected and contracts are ready to be executed will be grounds for disqualification of an otherwise successful bid.

Workers’ Compensation Requirements under WCL § 57:

To assist state and municipal entities in enforcing WCL §57, businesses requesting permits, licenses or seeking to enter into contracts must provide ONE of the following forms to the entity issuing the permit or entering into a contract:

- Certificate of Attestation of Exemption from NYS Workers' Compensation and/or Disability Benefits Coverage (CE-200); or
- Certificate of Workers' Compensation Insurance (C-105.2) (the business' insurance carrier will send this form to the government entity upon request) Please Note: The State Insurance Fund provides its own version of this form, the U-26.3; or
- Certificate of Worker's Compensation Self-Insurance (SI-12) (the business calls the Board's Self- Insurance Office at 518-402-0247); or
- Certificate of Group Worker's Compensation Self-Insurance (GSI-105.2) (the business' Group Self- Insurance Administrator will send this form to the government entity upon request).

Effective September 9, 2007, all out-of-state employers with employees or subcontractors working in New York State are required to carry a full, statutory New York State workers' compensation insurance policy.

An employer has a full, statutory New York State workers' compensation insurance policy when New York is listed in Item "3A" on the Information Page of the employer's workers' compensation insurance policy. Please contact the Board's Bureau of Compliance at 1-866-298-7830 if you have any questions regarding these requirements.

Please note: If all work for the permit, license or contract is done outside of New York and no employees of the out-of-state business work in the state, New York State-specific coverage is not required and the employer may be able to file Form CE-200.

Disability Benefits Requirements under WCL § 220(8):

To assist state and municipal entities in enforcing Sec. 220 Subd. 8 of the New York State Disability Benefits Law, businesses requesting permits, licenses or seeking to enter into contracts must provide one of the following forms to the government entity issuing the permit, license or entering into a contract:

- Certificate of Attestation of Exemption from NYS Workers' Compensation and/or Disability Benefits Coverage (CE-200); or
- Certificate of NYS Disability Benefits Insurance (DB-120.1) (the business' disability benefits carrier will send this form to the government entity upon request)
- Certificate of NYS Disability Benefits Self-Insurance. (DB-155) (businesses that are self-insured in NYS for disability benefits insurance should call the Workers' Compensation Board's Self-Insurance Office at (518) 402-0247 to obtain this form.)

Please note: New York State statutory disability benefits (DB) insurance coverage is totally different from and is not included in New York State workers' compensation insurance coverage. Statutory New York State disability benefits insurance covers employees for an off-the-job accident, injury or illness and pays half an employee's weekly wage, up to \$170 per week, for up to 26 weeks.

An out-of-state employer needs a New York State disability benefits insurance policy if the employer employs one or more individuals on each of at least 30 days in a calendar year in New York State. To be eligible for a disability benefits exemption using Form CE-200, an out-of-state employer must not have one or more individuals working on each of at least 30 days in a calendar year in New York. (Independent contractors are not considered to be employees under the Disability Benefits Law.)

If you have any additional questions regarding workers' compensation coverage requirements, please call the Bureau of Compliance at (866) 298-7830.

Obtaining Workers' Compensation and Disability Benefits Insurance

It may be appropriate to check the yellow pages, contact your insurance broker, carrier or agent, check with your trade association, or conduct additional research to find the most appropriate insurance coverage for your company. In addition, a workers' compensation policy may be obtained from the NYS Insurance Fund by calling 1-888-875-5790 and a disability benefits insurance policy may be obtained from the NYS Insurance Fund by calling 1-866-697-4332.

L. Maintenance Bond

The Contractor shall post and keep in effect throughout the term of the Contract, a faithful performance bond to secure the maintenance and repair responsibilities required by the Contract and by agreements for Authorized User locations under the jurisdiction of the Contract.

For each year that the Contractor is obligated to perform maintenance, the bond shall be furnished in a sum equal to a mutually agreeable reasonable estimate of the Contractor's annual maintenance and repair responsibilities based upon the annual maintenance plan furnished at the commencement of the Contract. The Contractor's initial Annual Maintenance Plan and estimate of annual maintenance costs for the PSCTS shall be set forth in the proposal as specified in Attachment 24.

The maintenance bond shall be from a surety and in a form that has been approved in advance, by the State and shall name the State as an irrevocable beneficiary of any portion or the full amount which will entitle the State to proceed against the bond upon the failure of the Contractor to provide the planned and unplanned maintenance required under this Contract. A copy of the maintenance bond shall be promptly forwarded to NYS and/or other State officials.

5.9 Title & Legal Interests

A. Documentation

The State shall own title to all drawings, documentation, technical designs and specifications (including but not limited to bid proposals, engineering drawings, plans, reports, training, maintenance or operating manuals), including network design, equipment configurations and documentation, whether preliminary, final or otherwise and may reproduce same for its own use. The Contractor shall deliver to the possession of NYS all work-in-progress documentation as it becomes available, but in no event later than thirty (30) calendar days after creation.

B. Incorporation into Subcontracts

The Contractor shall incorporate all of the provisions hereof respecting Title and Legal Interests in Documentation, and PSCTS Infrastructure into subcontracts entered into by the Contractor in connection with performance of Contractor's obligations under the terms of this RFP and resulting Contract. Other than as set forth above and with express written approval of the State, the Contractor shall not sell, assign, encumber, lien or otherwise pledge PSCTS Infrastructure as collateral for any obligations or indebtedness of the Contractor.

5.10 Submission of Contractor Invoices

It is agreed that payments are to be made by DCJS or any other applicable State agency in accordance with the terms and conditions of the payment schedule outlined in Section 3.2 of the RFP and Contractor's RFP response, or as otherwise mutually agreed by the parties. Contractor shall submit any invoices associated with a specific project deliverable at the completion of that activity. All payments from the State shall be made: (i) upon certification by the applicable State Agency Project Director or other designated State employee that the work invoiced by such invoice has been satisfactorily performed pursuant to the terms of this Contract, and (ii) upon submission of invoices satisfactory to the Comptroller of the State of New York in compliance with State Finance Law requirements.

5.11 Payment for Services of Contractor

Contractor shall provide complete and accurate billing invoices to the applicable State agency in order to receive payment. Billing invoices submitted to the agency must contain all information and supporting documentation required by the Agreement, the State agency and the State Comptroller. Payment for invoices submitted by the Contractor shall only be rendered electronically unless payment by paper check is expressly authorized by the head of such State agency, in his/her sole discretion, due to extenuating circumstances. Such electronic payment shall be made in accordance with ordinary State procedures and practices. The Contractor shall comply with the State Comptroller's procedures to authorize electronic payments. Authorization forms are available at the State Comptroller's website at www.osc.state.ny.us/epay/index.htm, by email at epunit@osc.state.ny.us, or by telephone at 518-474-4032. Contractor acknowledges that it will not receive payment on any invoices submitted under this Agreement if it does not comply with the State Comptroller's electronic payment procedures, except where the head of the State agency has expressly authorized payment by paper check as set forth above. It is further understood that the State shall only make payment upon the signed acceptance of project scheduled deliverables by an authorized DCJS or other State agency representative.

5.12 Warranties

In addition to the warranties set forth elsewhere in the Contract, the following warranties **shall survive beyond termination or expiration of the Contract** term in accordance with the terms below. Contractor, in submitting its Bid Proposal and executing the Contract, warrants and represents to the State the following:

A. Public Safety Credentialing and Training System Performance

Contractor warrants that all components or deliverables specified and furnished by or through the Contractor under this Contract meet the requirements set forth in the RFP and any subsequent Statement(s) of Work (SOW), and that services will be provided in a workmanlike manner in accordance with industry standards. Contractor warrants and represents that the PSCTS shall operate in accordance with the requirements and acceptance criteria set forth in the Contract. If any portion of the PSCTS fails to meet this warranty standard, the Contractor shall repair or replace the defective component at its sole expense to minimize disruption and loss of functionality, time being of the essence.

Contractor warrants and represents full ownership, clear title free of all liens, and/or that Contractor has obtained on behalf of NYS perpetual license rights set forth herein to use the Contractor's proposed PSCTS solution including equipment, software, customizations and services ("Product"), for the purposes stated in Section 1.4 of the RFP. Contractor shall indemnify NYS for any loss, damages or actions arising from a breach of this warranty without limitation. NYS may require Contractor to furnish appropriate written documentation establishing the above rights and interests as a payment. NYS' request or failure to request such documentation shall not relieve Contractor of liability under this warranty.

Contractor warrants and represents that any required deliverables specified and furnished by or through Contractor, whether tangible or intangible, regardless of form, shall be standard new equipment, current model or most recent release of regular stock product with all parts regularly used with the type of equipment offered, with no attachment or part substituted or applied contrary to the manufacturer's recommendations and standard commercial practice in the industry.

Contractor warrants and represents that all Products or deliverables specified and furnished by or through Contractor under the Contract meet the completion criteria set forth in the Contract and any subsequent SOW, and that services will be provided in a workmanlike manner in accordance with industry standards, as applicable.

Contractor further warrants and represents that Products or deliverables specified and furnished by or through the Contractor under the Contract shall individually, and where specified by Contractor to perform as a system, be substantially uninterrupted and error

free in operation and guaranteed against faulty material and workmanship for the warranty period stated in the Contract, or a minimum of eighteen (18) months from the date of acceptance, whichever period is longer ("Project Warranty Period"). During the Project Warranty Period, defects in the Products or deliverables specified and furnished by or through Contractor shall be repaired or replaced at no cost or expense to NYS.

Contractor shall extend the Project Warranty Period for individual Product(s) or for the PSCTS as a whole, if applicable, by the cumulative period(s) of time, after notification, during which an individual Product or the PSCTS requires servicing or replacement (down time), or is in the possession of the Contractor's subcontractors, distributors, resellers or employees.

In addition to Contractor's Project Warranty; NYS shall have the benefit of all manufacturers' standard commercial warranties for individual project deliverables. It shall be the Contractor's responsibility to insure such warranties begin conterminously with the commencement of Contractor's Project Warranty Period. Any additional cost(s) for having the periods begin conterminously shall be borne by the Contractor. During the Project Warranty Period, Contractor shall be responsible for placing and coordinating all manufacturers' warranty claims on behalf of NYS. Such manufacturer's warranty coverage shall be supplemental to, and not relieve the Contractor from its warranty obligations during the Project Warranty Period.

Where the manufacturer's warranty term is longer than the Project Warranty Period, Contractor shall notify NYS and pass through the manufacturer's warranty to NYS at no additional charge. Contractor shall not be responsible for coordinating services under the manufacturer's warranty after expiration of the Project Warranty Period.

B. Conformance to Manufacturer's Specifications

The warranties expressly set forth in this RFP and resulting Contract will be in lieu of all other warranties, express or implied including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The above warranties do not apply to the extent the problem is caused by misuse, unauthorized modification, unsuitable physical environment, failure to follow required maintenance by the NYS or failure caused by product for which the Contractor is not responsible.

C. Product & Equipment Warranty

At all times during the Contract term, Contractor warrants and represents that the Product delivered under this Contract conform to the requirements, specifications, performance standards and documentation, and the documentation fully describes the proper procedure for use. Technologies and equipment offered shall be standard new equipment, current model or most recent version or release of standard commercial offering with all parts regularly used with the type of equipment offered; and no attachment or part has been substituted or applied contrary to the manufacturer's recommendations and standard practice.

Contractor further warrants and represents that the Product delivered under this Contract (including any equipment, components or deliverables specified and furnished by or through Contractor) shall individually, and where specified and furnished as a system, be substantially uninterrupted or error-free in operation and guaranteed against faulty material and workmanship for the manufacturer's standard warranty period or for the duration of the Contract, whichever is longer ("warranty period"). During the warranty period, defects in the materials or workmanship of components or deliverables specified and furnished by or through Contractor shall be repaired or replaced by Contractor at no cost or expense to the State.

If during the warranty periods faults develop, the Contractor shall promptly repair or, upon demand, replace the defective unit or component part affected. Substituted or replacement Product shall be unconditionally guaranteed for a period of one year from the date such substituted or replacement Product was installed or replaced, the standard manufacturer's warranty period, or the remaining duration of the warranty period, whichever is longer.

Where third party equipment manufacturer or software developer offers any project deliverable by or through Contractor with a standard commercial warranty, such standard warranty shall be in addition to, and not relieve the Contractor from, Contractor's warranty obligations during the project warranty period(s). Where a standard commercial warranty covers all or some of the warranty period(s), Contractor shall be responsible for coordinating the warranty service with the third party manufacturer(s) or developers.

All costs for labor and material and transportation incurred to repair or replace defective Product during the warranty period shall be borne solely by the Contractor, and the State shall in no event be liable or responsible therefore.

D. Title & Ownership Warranty

Contractor warrants and represents full ownership, clear title free of all liens and encumbrances, and/or that Contractor has obtained on behalf of the State perpetual license rights to use the Police Peace Registries Product, hardware, interfaces, third-party software or any other deliverable ("System") pursuant to this Contract. Contractor shall be solely liable for any costs of acquisition associated therewith. Contractor fully indemnifies the State for any loss, damages or actions arising from a breach of said warranty without limitation. The State or DCJS ("Authorized Police Peace Registries User") may require Contractor to furnish appropriate written documentation establishing the above rights and interests as a condition of Contract award or payment. The State's request or failure to request such documentation shall not relieve Contractor of liability under this warranty.

E. Contractor Compliance

Contractor warrants and represents that it will pay, at its sole expense, all applicable permits, licenses, tariffs, tolls and fees and gives all notices and complies with all laws, ordinances, rules and regulations of any governmental entity in conjunction with the performance of obligations under the Contract. Prior to award and during the Contract term and any renewals thereof, Contractor shall establish to the satisfaction of the State that it meets or exceeds all requirements of the bid/ Contract and any applicable laws, including but not limited to, permits, insurance coverage, licensing, proof of coverage for workman's compensation, and shall provide such proof as required by the State. Failure to do so may constitute grounds for the State to cancel or suspend this Contract, in whole or in part, or to take any other action deemed necessary by the State.

F. Virus Warranty

Contractor warrants and represents that licensed or customized Software contains no known viruses.

G. Workmanship Warranty

Contractor warrants and represents that all components or deliverables specified and furnished by or through Contractor under the Contract meet the completion criteria set forth in the Contract and any subsequent statement(s) of work, and that services will be provided in a workmanlike manner in accordance with industry standards.

H. Adequate Parts Supply

Contractor warrants and represents that adequate parts supply will be available throughout the term of the Contract and extensions and stored in such locations to meet the response times and performance specifications set forth herein.

I. Date Processing Warranty

Contractor warrants and represents that Contract services involving the processing of date/time data shall be provided in an accurate and timely manner insofar as accurately processing date/time data, including leap year calculations. In the event of any breach of this warranty, the Contractor shall restore the services to the same level of performance as warranted herein, and clean, repair or replace data, time being of the essence, at the Contractors' sole cost and expense.

The Contractor shall, at its sole cost and expense, promptly repair or, upon demand, replace the defective unit or component part affected or furnish a patch or temporary fix or work around during the period in which the repair is made so that the performance and functionality of the PSCTS is maintained, time being of the essence.

All costs for labor and material and transportation incurred to repair or replace defective equipment or components during the warranty periods shall be borne solely by the Contractor, and the State shall in no event be liable or responsible therefore.

The Contractor shall provide a warranty period of eighteen months from the date of system acceptance for all products and deliverables. This warranty period shall include full maintenance services at no additional cost to NYS. The Contractor shall include details of the proposed warranty to meet NYS' needs as described in this RFP.

J. Personnel Eligible for Employment

The Contractor further warrants to NYS that contractor personnel performing services under the Contract are eligible for employment in the United States.

K. Survival of Warranties

All warranties contained in the Contract shall survive the termination of the Contract. The Contractor will maintain all original manufacturers' warranties and will present the organized warranty package to NYS and any other State official or employee upon completion and/or termination of contract, as requested.

5.13 Indemnification & Limitation of Liability

- A. Contractor shall be fully liable for the actions of its agents, employees or subcontractors and shall fully indemnify and save harmless the State and DCJS from suits, actions, damages and costs of every name and description for acts or omissions including but not limited to those relating to personal injury and damage to real or personal tangible property caused by Contractor, its agents, employees, subcontractors, *without limitation*; provided, however, that the Contractor shall not indemnify for that portion of any claim, loss or damage arising hereunder arising from the negligence of NYS or any of its employees.
- B. Contractor will indemnify, defend and hold the State harmless, *without limitation*, from and against any and all damages, losses, expenses (including reasonable attorneys' fees), claims, judgments, liabilities and costs which may be finally assessed against the NYS, any other State agency, and/or the State as a whole in any action for infringement of a patent with respect to the Product furnished, or of any copyright, trademark, trade secret or intellectual property right, provided that the Contractor receives: (i) prompt written notice of any action, claim or threat of infringement suit, or other suit, (ii) the opportunity to take over, settle or defend such action, claim or suit at Contractor's sole expense, and (iii) assistance in the defense of any such action at the expense of Contractor. Where a dispute or claim arises relative to a real or anticipated infringement, the Contractor may be required at its sole expense, to submit such information and documentation, including formal patent attorney

opinions, as NYS, another State entity, including the Department of Law shall require. If the Contractor has an opportunity to terminate any such infringement suit by a third-party Contractor, the Contractor shall obtain the consent of NYS, the State and the Attorney General of the State of New York to the settlement if such settlement will alter any financial or performance terms of the Agreement.

1. If principles of governmental or public law are involved, NYS and the State may participate in the defense of any such action, but no costs or expenses shall be incurred for the account of the Contractor without its written consent.
2. If in the Contractor's opinion the equipment, materials, or information mentioned in paragraph b., above, are likely to or do become the subject of a claim of infringement of a United States patent or copyright, then without diminishing the Contractor's obligation to satisfy any final award, Contractor may, with NYS, and the State's written consent, substitute other equally suitable equipment, materials, and information or, at Contractor's option and expense, obtain the right for the State to continue the use of such equipment, materials, and information.

C. The Contractor will indemnify NYS and the State *without limitation* against any claims brought against NYS and/or the State by reason of a wrongful disclosure of confidential information attributed to the Contractor or any of its agents, employees, and/or subcontractors and will cooperate fully with NYS, the State, and the Attorney General in defense of any claim(s).

D. The Contractor shall not be obligated to indemnify that portion of a claim or dispute based upon: i) unauthorized modification or alteration of a product; ii) use of the product in combination with other products not furnished by Contractor; iii) use in other than the specified operating conditions and environment.

E. Neither party shall be liable for any delay or failure in performance beyond its control resulting from acts of God or force majeure. All parties shall use reasonable efforts to eliminate or minimize the effect of such events upon performance of their respective duties under the Contract and shall immediately resume performance upon termination of the force majeure.

F. Unless otherwise specifically enumerated herein, neither party shall be liable to the other for special, indirect or consequential damages, including lost data or records (unless the Contractor is required to back-up the data or records as part of the work plan), even if the party has been advised of the possibility of such damages. Neither party shall be liable for lost profits, lost revenue or lost institutional operating savings. Indemnification for Direct Damage: For all other claims against the Contractor where liability is not otherwise set forth in the Contract as being "without limitation" and regardless of the basis on which the claim is made, Contractor's liability under this Contract for direct damages shall be two (2) times the charges rendered by the Contractor under the Contract.

G. NYS and the State may, in addition to other remedies available to them at law, in equity, or under the Contract, and upon notice to the Contractor, retain such monies from amounts due Contractor, or may proceed against the maintenance bond, , as may be necessary to satisfy any claim for damages, costs and the like asserted by or against them.

5.14 Software, Customizations Upgrades

Software error corrections, revisions, feature enhancements or upgrades for products delivered under this Contract, including the PSCTS, will be provided at no charge by the Contractor during the Contract term and shall be made available throughout the life of the Contract, including any contractual amendment, at no additional charge other than the pricing set forth in the Contract, unless otherwise agreed in writing by DCJS/State.

The Contractor will be required to notify the State immediately of the availability of software upgrade(s). Implementation of an upgrade is at the sole discretion of the State, provided, however, that the non-implementation of any software upgrade does not substantially impair system performance or reliability.

A. Software License

Title and ownership to proprietary commercial software delivered under the Contract shall remain with the proprietary owner(s) (“Licensor”). Effective upon delivery, such software shall be perpetually licensed to the State. Licensor may not terminate the use of the Product in ways which would otherwise be prohibited by law (“License”) without first providing DCJS/State with written notice of the material breach giving rise to the termination and a thirty (30) calendar day opportunity to cure.

B. Archival Back-up for Licensed Software

The Contractor shall copy and retain the licensed software and related documentation for all software and upgrades for the purpose of 1) trouble shooting diagnostic; 2) reproducing copies of the Licensed Product for archival backup and disaster recovery procedures in the event of destruction or corruption of the software or disasters or emergencies which require PSCTS to restore backup(s) or to initiate disaster recovery procedures for its platform or operating systems; and 3) reproducing a reasonable number of copies of the Product and related documentation for cold site storage. “Cold Site” storage shall be defined as a restorable back-up copy of the Product not to be installed until and after the declaration by the State of a disaster.

C. Transfers or Assignments to a Third Party Agent

The State may assign or transfer its rights in licensed software to a third party entity or trustee (“Trustee”).

D. Confidentiality

Licensed software is considered a trade secret, copyrighted and proprietary product. The State will not disclose or otherwise distribute or reproduce any licensed software to anyone other than as authorized under the terms of Contract. The State will not remove or destroy any proprietary markings of Contractor. Except as expressly authorized by the terms of license, the State shall not:

1. Copy the Product;
2. Cause or permit reverse compilation or reverse assembly of all or any portion of the Product;
3. Export all or any portion of the Product in violation of any U.S. Department of Commerce export administration regulations.

5.15 Escrow for Software Source Code

Contractor shall establish and maintain, at its expense, an established escrow agreement in effect in perpetuity for the original installed and every subsequent version of the source code, including proprietary code, to the software delivered under the Contract ("Source Code"). The Contractor shall establish procedures to continually update the Source Code, including any change in the proprietary code, as new versions of the software are implemented into production.

A. Escrow

The Contractor shall provide in writing to DCJS' Procurement Officer or such State official or employee designated for such purpose, the name and contact address/phone number of the neutral third party ("Escrow Agent") holding, in trust, all original installed and subsequent versions of the Source Code, including proprietary code, designated to the State. The escrow agreement has to name DCJS and the State of New York as an irrevocable beneficiary, and the State of New York acting on behalf of Authorized PSCTS User(s) of this Contract. The escrow agreement may not be terminated by either Contractor or the Escrow Agent without prior written approval by the State. Throughout the term of the Contract, Contractor shall be obligated to annually update and appropriately identify the deposited materials, including current versions of the source code for the most recent release, error corrections, enhancements or updates of software delivered under this Contract.

B. Terms of Escrow

The Contractor's Escrow Agent shall provide annual written notice to the State that such escrow is in effect, and shall notify in writing the State as to the version or releases held by such agent by providing the contents list for the escrow. The Escrow Agent shall,

during the term of the escrow agreement, periodically inspect the deposit materials and compare them with the contents list for the escrow. The Escrow Agent may not raise any defenses against the State that the agent may have against the Contractor to restrict the release of source code to the State. The escrow agreement shall not include any provisions relating to the release of the escrow contents that would require, prior to release, the State to submit to arbitration. The escrow agreement shall require the Escrow Agent to provide the following notices and to release the escrow as follows:

1. Required Notice to State from Escrow Agent:

The Escrow Agent is required to furnish written notice(s) to DCJS' Procurement Officer (at the address for notices set forth in this RFP, Section 5.8) upon the happening of any one or more of the following events:

- a. Failure of Contractor to pay required escrow fees;
- b. Voluntary termination or transfer of escrow account by Contractor;
- c. Entry of an order for relief under Title 11 of the United States Code against Contractor, or any involuntary order;
- d. The making of a general assignment by Contractor for the benefit of creditors;
- e. The appointment of a general receiver or trustee in bankruptcy of Contractor's business or property;
- f. Action by Contractor under any state insolvency or similar law for the purposes of its bankruptcy, reorganization or liquidation;
- g. Court ordered liquidation against Contractor; or
- h. Contractor's failure to update the Source Code and/or to deposit new code with Escrow Agent at least annually after the effective date of the escrow.

2. Requirement for Release of Source Code

The terms of escrow shall provide for release of the source code upon the happening of one or more of the following events:

- a. Failure of Contractor to carry out PSCTS ongoing maintenance or support obligations set forth in this Contract;
- b. Failure of Contractor to continue to do business in the ordinary course;
- c. Existence of any one or more of the following circumstances, if uncorrected for more than sixty (60) calendar days:
 - i. entry of an order for relief under Title 11 of the United States Code;
 - ii. the making by the Contractor of a general assignment for the benefit of creditors;
 - iii. the appointment of a general receiver or trustee in bankruptcy of Contractor's business or property; or action by the Contractor under any state insolvency or similar law for the purposes of its bankruptcy, reorganization, or liquidation.

The occurrence of the described events will not constitute a release condition if, within the specified sixty (60) calendar day period, Contractor (including its assignee or its

receiver or trustee in bankruptcy) provides to the State adequate assurances, reasonably acceptable to the State as solely determined by State, of its continuing ability and willingness to fulfill all of its maintenance and support obligations. Additionally, if the State feels that a condition for release has occurred, the State shall notify the Escrow Agent, who shall notify Contractor of the intended release. Contractor has a maximum of fifteen (15) business days to object to the release. If an objection is filed, the Escrow Agent shall continue to retain the source code until otherwise directed by mutual agreement of the parties or until otherwise directed by a court of competent jurisdiction. Notwithstanding the foregoing, if after an objection has been filed, the State certifies in writing an “emergency”, as defined below, has occurred, the Escrow Agent shall immediately release the source code to the State. An “emergency” shall be defined as the State’s written certification that, the State reasonably believes that a feature in the Contractor’s product has caused the system to crash and render it inoperable and the Contractor has refused to provide remedial assistance to correct the failure within five (5) business days from receipt of written notice, via e-mail, of the failure and such condition requires an immediate release of the source code for State’s internal use to correct the failure in order to continue normal system operation and full functionality. Upon release of the Source Code, the State may release the Source Code to the Authorized PSCTS User(s), if necessary, for remedial maintenance purposes only.

C. Changes in Escrow

The escrow agreement shall designate the State as a “co-party”, which is entitled to receive notice from the agent if there is any change in the status of the escrow agreement between Contractor and the agent, including notice of a proposed termination or transfer. Before the Contractor can change a designated Escrow Agent, the Escrow Agent and the Contractor shall provide the State a minimum advanced notice of sixty (60) business days of the proposed change. Before the escrow may be moved or changed, the State has to be notified of the identity of the new proposed agent, and the new agent has to confirm the same terms of escrow vis-à-vis the State’s interests.

5.16 Compliance with Miscellaneous Laws

To the extent that DCJS and/or the State is the recipient of any federally funded monies relating to the procurement of Services or Products under the RFP and Contract, Contractor agrees to comply with all applicable federal laws, rules and regulations including but not limited to the following areas as further set forth at Chapters II and XXX of 7 CFR and 45 CFR Parts 74 and 95 relating to:

- a. Equal Employment Opportunity as set forth in federal Executive Orders 11246 and 11375 as supplemented by 41 CFR 60, and the nondiscrimination requirements of 45 CFR Parts 80, 84 and 90, and 7 CFR Parts 15, 15b and 15d.
- b. Copeland "Anti-Kickback Act" (18 USC 874 and 40 USC 276c) which provides that all contracts/subgrants greater than \$2,000 for construction or repair must have a provision requiring compliance with 18 USC 874 as supplemented by 29 CFR Part 3,

which prohibit contractors or sub recipients from inducing by any means any person employed in construction, completion or repair of public work to give up any part of compensation to which they are otherwise entitled and that the recipient shall report all suspected/reported violations to the Federal awarding agency.

c. Davis-Bacon Act, as amended (40 U.S.C. 276a to a-7) which requires all construction contracts awarded by recipients of more than \$2000 to comply with the Act as supplemented by USDOL Regulations 29 CFR Part 5 requiring all contractors to pay wages to laborers and mechanics at a rate not less than the minimum wage specified by the Federal Secretary of Labor, which wages shall be paid not less than once a week. The recipient shall place a copy of the federally specified wage (the "prevailing wage") in each solicitation and the award of a contract shall be conditioned upon acceptance of such a determination. The recipient must report all suspected/reported violations to the Federal awarding agency.

d. Contract Work Hours and Safety Standards Act (40 U.S.C. 327-333) which requires, where applicable, that all construction contracts and other contracts involving employment of mechanics and laborers require compliance with 40 U.S.C. 327-333 as supplemented by USDOL Regulations 29 CFR 5 when said contracts exceed \$100,000, which references require that work in excess of 40 hours/week be recompensed at a rate at least 50% greater than the basic pay rate and that no work be required in unsanitary, hazardous, or dangerous conditions. These requirements do not apply to the purchases of supplies, materials, or articles ordinarily available on the open market or contracts for transportation or transmission of intelligence.

e. Rights to Inventions Made under a Contract or Agreement- Contracts or Agreements for the performance of experimental, developmental, or research work shall provide for the rights of the federal government and the recipient in any in any resulting invention in accordance with 37 CFR Part 401 and any further implementing regulations issued by USDHHS or USDA.

f. Ownership Rights in Software or Modifications Thereof – The State shall have all ownership rights in software or modifications thereof and associated documentation designed, developed or installed with Federal financial participation, and the federal government reserves a royalty-free, nonexclusive, and irrevocable license to reproduce, publish, or otherwise use and to authorize others to use for Federal Government purposes, such software, modifications, and documentation, provided, however, that this sentence shall not apply to 'proprietary operating/vendor software packages' within the meaning of 45 CFR 95.617(c) and 7 CFR 277.18(l)(1)(iii).

g. Clean Air Act (42 U.S.C. 7401 et seq.) and the Federal Water Pollution Control Act as amended (33 U.S.C. 1251 et seq.), which require Contracts and subgrants in excess of \$100,000 shall require the recipient to comply with the Acts recited herein and that violations must be reported to USDHHS and the appropriate Regional Office of the Federal Environmental Protection Agency.

h. Byrd Anti-Lobbying Amendment (31 U.S.C. 1352)- which requires that every contractor under a contract for more than \$100,000 and every tier of contractors or subcontractors thereunder shall file certification, as required, that said contractor will not and has not used any Federal appropriated funds to pay any person or organization for influencing or attempting to influence any federal agency, member of Congress, or an employee of a member of Congress in connection with obtaining any Federal contract,

grant, or award covered by such Amendment. A contractor or subcontractor from any tier shall also disclose any lobbying with non-federal funds that takes place in conjunction with obtaining a federal award, which disclosure shall be forwarded up any applicable tiers to the recipient. (See also 45 CFR 93)

i. Debarment and Suspension. (Federal E.O.s 12549 and 12689)- Certain contracts shall not be awarded to parties listed on the non-procurement portion of the U. S. General Services Administration's "Lists of Parties Excluded from Federal Procurement or Nonprocurement Programs" in accordance with E.O.s 12549 and 12689. (See 45 CFR 76.) Contractors with awards that exceed the simplified acquisition threshold shall provide the required certification regarding their exclusion status and that of their principals prior to award.

j. Contractor shall make positive efforts to assure that small businesses and minority and women owned business enterprises (M/WBEs) are utilized when possible as sources of supplies, equipment, construction and services. If any subcontracts are to be let, Contractor shall (1) include qualified small businesses and M/WBEs on solicitation lists; (2) assure that they are solicited whenever they are potential sources; (3) when economically feasible, divide total requirements into smaller tasks or quantities so as to permit maximum small business and M/WBE participation; (4) where the requirement permits, establish delivery schedules which will encourage participation by small businesses and M/WBEs, and; (5) use the services and assistance of the New York State Department of Economic Development [(518) 292-5100, or its WebSite at www.esc.ny.gov,] the U.S Small Business Administration, the Office of Minority Business Enterprise of the US Department of Commerce and the U.S. Community Services Administration, as appropriate.

k. Contractor shall ensure that the contract provisions specified in 45 CFR 74.48 are included in all subcontracts.

In addition, the State shall adhere to and the Contractor and any of its subcontractors shall abide by Chapter 22 of the Laws of 2014, the Service-Disabled Veteran-Owned Business Act, and any regulations and/or applicable directives which may be adopted or implemented.

5.17 Termination

In addition to termination provisions heretofore specified in this RFP, the following additional termination provisions shall apply:

a. The Agreement may be terminated by mutual written agreement of the Parties.

b. This Agreement may be terminated by NYS, upon written notice if: Key Employees leave the employment of Contractor; the Contractor is adjudged bankrupt; the Contractor makes a general assignment for the benefit of creditors; a receiver is appointed due to the Contractor's insolvency; a petition in bankruptcy or insolvency is

filed, by or against the Contractor; or the Contractor persistently disregards laws, ordinances, rules, regulations or orders of any public authority having jurisdiction.

c. This Agreement may be terminated by NYS for cause upon the failure of the Contractor to comply with the terms and conditions of this Agreement, provided NYS gives the Contractor not less than thirty (30) calendar day's written notice and an opportunity to cure all items not in compliance with the terms and conditions of this agreement, including the attachments hereto. Termination shall be immediately effective upon receipt of such written notice. The Contractor agrees to incur no new obligations nor to claim for any expenses made after receipt of the notification of termination. Termination for cause shall create a liability upon the Contractor for legal damages.

d. This Agreement may be terminated without cause, for convenience or as may be determined by NYS to be in the best interest of the State, for reasons, including, but not limited to, changes in law or program administration and budgetary constraints. NYS shall give written notice to the Contractor not less than thirty (30) calendar days prior to the date upon which termination shall become effective. Such written notice shall be provided via registered or certified mail, return receipt requested or hand-delivered to the other party. The date of such notice will be deemed to be the date of postmark in the case of mail or the date of Contractor's receipt of notice in the case of hand delivery. In the case of termination under this section, NYS agrees to pay the Contractor for reasonable and appropriate expenses incurred in good faith. The Contractor agrees to incur no new obligations after receipt of notification of termination and to cancel as many outstanding obligations as possible.

e. NYS reserves the right to terminate this contract in the event it is found that any of the certifications filed by the Contractor with the State of New York were intentionally false or intentionally incomplete. Upon such finding, NYS may exercise its termination right by providing written notification to Contractor.

f. If NYS determines that funds are unavailable through lack of continued lawful appropriation therefore, NYS shall deem the Agreement terminated immediately. NYS agrees to give timely notice to the Contractor in the event of termination under this paragraph. If the initial notice is oral notification, NYS shall follow this up immediately with written notice. NYS will be obligated to pay the Contractor only for costs of pro rata services performed by the Contractor until such time as notice of termination is received either orally or in writing by the Contractor from NYS, or for other costs of pro rata services performed as otherwise mutually agreed by both parties.

g. In the event of termination for any reason, the Contractor shall not incur new obligations for the terminated portion and the Contractor shall cancel as many outstanding obligations as possible.

h. Termination under any provision of this Agreement shall not relieve the Contractor of any liability to NYS which it has under this Agreement, or for damages sustained by NYS by reason of any breach of this Agreement. NYS may withhold any

payments to the Contractor for the purpose of set-off until such time as the exact amount of damages due NYS from the Contractor is determined.

i. Termination of this Agreement, with or without cause, shall not create any liability on the part of NYS or the State for payment of any penalty, or any other liability.

General Responsibility Language

The Contractor shall at all times during the Contract term remain responsible. The Contractor agrees, if requested by the Commissioner of the New York State Division of Criminal Justice Services or his or her designee, to present evidence of its continuing legal authority to do business in New York State, integrity, experience, ability, prior performance, and organizational and financial capacity.

Suspension of Work (for Non-Responsibility)

The Commissioner of the New York State Division of Criminal Justice Services or his or her designee, in his or her sole discretion, reserves the right to suspend any or all activities under this Contract, at any time, when he or she discovers information that calls into question the responsibility of the Contractor. In the event of such suspension, the Contractor will be given written notice outlining the particulars of such suspension. Upon issuance of such notice, the Contractor must comply with the terms of the suspension order. Contract activity may resume at such time as the Commissioner of the New York State Division of Criminal Justice Services or his or her designee issues a written notice authorizing a resumption of performance under the Contract.

Termination (for Non-Responsibility)

Upon written notice to the Contractor, and a reasonable opportunity to be heard with the Commissioner of the New York State Division of Criminal Justice Services or staff, the Contract may be terminated by Commissioner of the New York State Division of Criminal Justice Services or his or her designee at the Contractor's expense where the Contractor is determined by the Commissioner of the New York State Division of Criminal Justice Services or his or her designee to be non-responsible. In such event, the Commissioner of the New York State Division of Criminal Justice Services or his or her designee may complete the contractual requirements in any manner he or she may deem advisable and pursue available legal or equitable remedies for breach.

In addition to the termination language related to responsibility above, the Commissioner in his sole discretion reserves the right to terminate this Agreement, with or without cause, at any time, for convenience or as may be in the best interests of the State. Termination of the Agreement, with or without cause, shall not create any liability on the part of NYS or the State for payment of any penalty, or any other liability.

A. For Convenience

The State hereby reserves the right to terminate this Contract for convenience, or in the event that necessary and lawful appropriations are not provided or continued for the funding of this contract by the Legislature or Governor subject to and in accordance with the following provisions:

1. The State shall have the right to unilaterally terminate this Contract, in whole or in part, for convenience provided that prior notice of such termination is given. Such option may be exercised upon thirty (30) calendar days advance written notice to the Contractor pursuant to paragraph (C), below. In the event that the State exercises this option, the Contract shall terminate as to the portion(s) of work being deleted as of the termination date set forth in paragraph (C), below, with obligations of the parties as follows:
 - a. The Contractor shall deliver to the possession of the State within such thirty (30) calendar day notice period all drawings, reports or other required Contract deliverables to date related to the portion(s) of work subject to the termination, whether preliminary or final, in the form and format set forth in this agreement. The State's receipt of such deliverables shall be a condition precedent to the obligation of the State to make payments to the Contractor.
 - b. Upon receipt of such deliverables, the State shall be obligated to pay the Contractor the amounts then due and owing as specified in the Contract as the exclusive amounts due Contractor, calculated as of the termination date, such payment to be tendered to Contractor within ninety (90) business days of receipt of the deliverables. The State shall not be liable to Contractor for lost profits, administrative or other expenses, however denominated.

B. For Cause

1. Notice

If either party fails to materially comply with any provision of the Contract the other party shall so notify the party in default as provided in paragraph (C), below. The notification shall specify in reasonable detail the nature of the default.

2. Cure Period

Where timeframes for performance are otherwise set forth in this Contract, the specific time period stated shall govern. For all other instances constituting Contractor's default, the Contractor shall have thirty (30) calendar days from the date of receipt of notice to correct the default ("cure period"). During the cure period, Contractor shall work diligently to resolve and cure any default. The State may, at its discretion, agree to extend the timeframe for cure.

Because of the secure nature of the Police Peace Registries, the State may, upon written notice to the Contractor, shorten the aforementioned thirty (30) calendar day cure period as it deems necessary in the event that the Contractor's breach threatens or has the potential to threaten the ongoing operation of the Police Peace Registries, or the health, safety or welfare of those served by the Police Peace Registries.

3. Default

If the Contractor is unable to cure the default within the cure period, in addition to availing itself of specific remedies set forth in the Contract, the State may pursue all legal and equitable remedies for breach. A delay or failure in declaring a material breach under this paragraph shall not be deemed a waiver of the right to subsequently declare a default.

4. Additional State Rights & Remedies

- a. In the event of Contractor's default, in addition to pursuing any other legal or equitable remedies, the State shall have the right to take one or more of the following actions:
 - i. terminate the Contract, in whole or in part;
 - ii. proceed against any Bond or Insurance furnished by Contractor or subcontractor, in accordance with the terms thereof;
 - iii. suspend, in whole or in part, payments due Contractor under this or any other New York State Contract;
 - iv. pursue equitable remedies to compel Contractor to perform; and/or v. all rights set forth under b, below.
- b. It is expressly understood between the parties that the State is contracting with Contractor for the personal services of Contractor in building, operation and maintenance of a PSCTS and associated network which is a public safety system operated and maintained by the State for the best interests of the State and safety and welfare of the citizens of New York.

Therefore, in the event of termination of this Contract in whole or in part based upon the Contractor's default or abandonment, the State shall, in its sole judgment, among other factors, determine the usability to the State of that portion of the PSCTS completed prior

to default with reference to completion of the foregoing mission. The State may, in accordance with that determination, pursue any remedies as it deems advisable in completing that mission, with sole reference to the best interests of the State, including, but not limited to:

- i. buy out all or part of the completed PSCTS or system components;
- ii. Contractor to license or grant to the State such intellectual property and patent rights for the proposed technology solution as are required for:
 - a) Continued operation and maintenance of the previously completed portion of the PSCTS, by the State or by a qualified third party selected by the State for the remainder of the original contract term, and/or;
 - b) the design, build, continued operation and maintenance of the uncompleted PSCTS deliverables due under the Contract;
- iii. procuring from any third party, upon such terms and in such manner as the State deems appropriate, either:
 - a) an alternate system(s) to complete the unfinished portion of the PSCTS deliverables at time of default, and/or;
 - b) pursuing any other action(s) provided at law or in equity as the State deems necessary to enable the State to complete the above mission.

The Contractor shall be liable for any and all excess costs for remedies pursued by the State, and for administrative costs incurred by the State in procuring alternate services.

5. Transition

In the event that the PSCTS is operational at the point that a termination for cause is issued, the Contractor shall provide and comply with the requirements for transition set forth in Section 5.18, below.

6. Cumulative Remedies

The rights and remedies provided in this paragraph are cumulative to and in addition to any other rights and remedies provided by law, at equity, or under the Contract.

C. Termination Notice

Notices required by this section shall be delivered to the other party in writing, by certified mail, return receipt requested. The date of notice shall be deemed the date of

delivery set forth on the return receipt. (“date of return receipt notice”) Such notice shall be addressed as follows:

State of New York:

Commissioner
Division of Criminal Justice Services
Alfred E. Smith Building, 8th Floor
80 South Swan Street
Albany, NY 12210

Contractor:

D. Termination Date

Contract termination dates shall be determined as follows:

In the event a notice of termination is issued for convenience, the Contract termination date shall be deemed ninety (90) calendar days from the date of delivery set forth on the return receipt notice.

Subject to the State’s right to shorten the cure period pursuant to paragraph (B), above, in the event a notice of termination is issued for cause, the Contract termination date shall be from the date of the return receipt notice, or such other extended period of time as has been mutually agreed in writing by the parties.

E. Mitigation of Costs

The Contractor shall not undertake any additional or new Contractual obligations on or after the date of return receipt notice of a termination notice without the prior written approval of the State. On or after the date of return receipt notice of a termination notice and during the termination notice period, the Contractor shall take all commercially reasonable and prudent actions to close out unnecessary outstanding, existing obligations as economically as possible for the State.

F. Asset Accounting & Transfer

Within thirty (30) calendar days of receipt of a termination notice, the Contractor shall be required to update and finalize a complete inventory of the PSCTS infrastructure, supplies, equipment and other tangible or intangible assets. (“assets”) To the extent that

such assets are subject to a financing or other lease agreement as of the date of notice, and that the State has exercised the purchase option as to such asset(s) or has elected to complete the PSCTS mission in accordance with Section 5.14 (C), above, the State may require Contractor to execute all necessary and appropriate legal documents evidencing a transfer of ownership or assignment of Contractor's interest in such assets to the State or other third party designated by the State as the State or Contractor's successor in interest.

5.18 Post Termination Transition

Because of the public safety interests of the State, the State may require the Contractor to provide uninterrupted services after Contract termination as the State deems reasonable and necessary for the continued safe operation of the PSCTS and/or as necessary for the State to comply with all legal requirements for establishing a new Contract to continue safe operation of the PSCTS ("transition period"). Transition services shall be governed as follows:

A. Post Termination Transition Period

The post termination transition period shall be determined by the State, and set forth in writing, return receipt notice, to the Contractor. The State shall consult with the Contractor prior to making such determination. The State reserves the right to subsequently amend the post termination transition period upon thirty (30) calendar days advance written notice to the Contractor.

B. No Interruption in Service

At all times during the post termination transition period and unless waived by the State, the Contractor shall continue all Contractual obligations set forth in the Contract until such time as the State (i) has approved the Contractor's proposed post termination transition plan, and (ii) an orderly post termination transition to the State or a new Contractor has been completed pursuant to the approved post termination transition plan. The Contractor shall be required to meet its Contractual obligations pursuant to this paragraph notwithstanding the issuance of a termination for cause.

C. Post Termination Transition Plan

Within fifteen (15) calendar days of receipt of a notice of termination as set forth elsewhere in the Contract or twelve months prior to the end of the term of the Agreement, whichever event occurs first, the Contractor shall provide for approval by NYS a detailed written plan for Post Termination Transition (Post Termination Transition Plan) which outlines, at a minimum, the tasks, milestones and deliverables associated with the smooth transition of the PSCTS to a successor Contractor, as applicable. Furthermore, the Post Termination Transition Plan must be amended by Contractor to include all other information deemed essential by the State, including development of specifications necessary for preparation of a competitive solicitation for the successor Contract.

D. Contractor Post Termination Transition Services

“Post termination transition services” shall be deemed to include Contractor’s responsibility for all tasks and services outlined in the Contract, and for transferring in a planned manner specified in the Post Termination Transition Plan all tasks and services to the State or successor Contractor. It is expressly agreed between the parties that the level of service during the post termination transition period shall be maintained in accordance with and shall be subject to all the terms and conditions of the Contract, provided, however, that where, during the post termination transition period, tasks or services are transitioned to or assumed by the State or the successor Contractor, Contractor shall not be held responsible for the acts or omissions of the State or successor Contractor or for service degradation resulting from the acts or omissions of the State or successor Contractor. The Contractor shall transfer to the successor Contractor all title, leasing rights, or license rights of all hardware and equipment in use in the PSCTS operation. The successor Contractor shall utilize such hardware and equipment in accord with the rights and duties attendant thereto. The Contractor shall turn over to the successor Contractor all network software, data files, application programs, and documentation.

E. Compensation for Post Termination Transition Services

Contractor shall be reimbursed for services performed during the post termination transition period at the rates previously set forth in the Contract.

F. State Responsibilities for Post Termination Transition

The State shall assume responsibility for post termination transition project management. A project manager responsible for coordinating post termination transition activities, maintaining the transition task schedule, and approving transition deliverables shall be appointed. Periodic project review meetings shall be held with representatives of the State, the Contractor, and the successor Contractor.

G. Training Successor Organization & Personnel

Post Termination Transition Services furnished by the Contractor must include the development of a training plan. The Contractor is required to provide post termination transition training for the successor organization’s management in the operation and maintenance of the PSCTS. The training effort shall focus on providing the successor Contractor’s management personnel with information about all operational aspects of the PSCTS. During transition, the Contractor shall prepare a detailed training program. This program shall establish a post termination transition training group which shall provide the required training for successor Contractor personnel.

Training shall be accomplished through a mixture of formal and on-the-job training. The successor Contractor's management personnel shall participate in all PSCTS related functions during the post termination transition period. The successor Contractor's management shall be asked to participate in normal operations and to fulfill required tasks. The Contractor agent shall also provide documented instructional materials to facilitate the learning process. The latest version of all documentation shall be used during the formal training sessions.

5.19 Rescale of Project

The State reserves the right to terminate or modify this Contract in the event of loss or change of funding streams or appropriations. The State reserves the option to rescale the capacity and/or functionality of the PSCTS or the contractual requirements in order to serve the best interests of the State. If the State exercises the option to reduce the scope, any proposed modifications to insure the performance or interoperability of the modified network will be subject to the Change Order provisions set forth in Section 5.20, below. If the State exercises the option to scale back the project, the State shall be entitled to a corresponding adjustment in fees due the Contractor with no further compensation due Contractor for any deleted scope.

5.20 Process for Change Orders

At any time during the term of this Contract, the State may make changes, subtractions or additions in any of the Equipment, Software, Documentation, Services and/or other Deliverables within the general scope of work set forth in the Contract, consistent with pricing established under the terms of this agreement. Such changes will be subject to the unit costs itemized in the Contract or such other costs as may be mutually agreed between the parties. All such changes shall be reduced to a written Change Order, Appendix J executed by both parties, and shall otherwise be in accordance with the terms and conditions of this Contract. The Change Order shall be accepted and agreed to by both the State and the Contractor as evidenced by the written signatures of the appropriate representatives of both parties. If any such change causes an increase or decrease in pricing or the time required for the performance of the Contract, an equitable adjustment of the Contract amount and/or time of performance will be made on mutual agreement of the parties, subject to the approval of the New York State Comptroller and any applicable control agency, if required.

5.21 Force Majeure

In the event of a service disruption caused by a Force Majeure which is outside of the control of either party, e.g., natural disaster, act of God, war, terrorism, civil disturbance, court order or labor dispute, ("force majeure") or any other acts beyond the reasonable control of either party, the party that has been so affected shall immediately give notice to the other party, and shall exercise every commercially reasonable effort to resume

performance, and an extension of the time for performance shall be granted for a period to be agreed to in writing by the State and Contractor.

In the event of a service disruption caused by a State Disaster Emergency, as defined in Section 20(2)(b) of the Executive Law or other emergency situation or occurrence that the Commissioner of the Division of Criminal Justice Services, the Governor, or any other State agency head in his or her sole discretion, has determined poses a risk to health and public safety or the conservation of public resources, the Contractor shall be notified that DCJS or the State is invoking this provision and that notwithstanding any other provision in the Contract, during a State disaster emergency or other emergency situation, unless the Contractor's performance would be excused pursuant to the *Force Majeure* provisions of the Contract, the Contractor shall provide the necessary Services to the State on a time-is-of-the-essence basis, working on a twenty-four (24) hour a day, seven (7) day a week basis, to restore and/or recover State operations and Services that are critical to the public safety, health, and welfare of the State, to be determined at the sole discretion of the State. Except as provided in this section, all other provisions of the RFP and Contract remain in full force and effect during a state disaster emergency or other emergency situation.

5.22 Press Releases

Contractor agrees that no brochure, news/media/press release, public announcement, memorandum or other information of any kind regarding the Contract shall be disseminated in any way to the public, nor shall any presentation be given regarding the Contract without the prior written approval by the undersigned or the undersigned's designee from DCJS or any other State entity where designated, which written approval shall not be unreasonably withheld or delayed provided, however, that Contractor shall be authorized to provide copies of the Contract and answer any questions relating thereto to any State or Federal regulators or, in connection with its financial activities, to financial institutions for any private or public offering.

5.23 Security, Information Security, Breach and Notification Act

The Contractor shall maintain the security, nondisclosure and confidentiality of all information in accordance with the following clauses in performance of its activities under the Contract. Contractor shall ensure that its personnel, agents, officers and any subcontractors are fully aware of the obligations arising under this section and shall take all commercially reasonable steps to ensure compliance. Disclosure of PSCTS information developed by the State, any Authorized PSCTS User, the Contractor or their employees, subcontractors, partners or its agents is strictly prohibited. The Contract may be terminated by the State for cause for a material breach of this section.

A. Security Procedures & Employee Dishonesty

Contractor warrants, covenants and represents that it will comply fully with all security procedures of the State in performance of the Contract. Contractor shall hold the State

harmless from any loss or damage to the State resulting from the violation by the Contractor, employees, and subcontractors of such security procedures or resulting from any criminal acts committed by such, employees, and subcontractors while providing services under the Contract.

B. Information Security Breach and Notification Act

Section 208 of the State Technology Law (STL) and Section 899-aa of the General Business Law (GBL) require that State entities and persons or businesses conducting business in New York who own or license computerized data which includes private information including an individual's unencrypted personal information plus one or more of the following: social security number, driver's license number or non-driver ID, account number, credit or debit card number plus security code, access code or password which permits access to an individual's financial account, must disclose to a New York resident when their private information was, or is reasonably believed to have been, acquired by a person without valid authorization. Disclosure of breach of that private information to all individuals affected or potentially affected must occur in the most expedient time possible without unreasonable delay, after necessary measures have been taken subject to approval of DCJS or such other applicable State agency to determine the scope of the breach and to restore integrity, but with delay if law enforcement determines it impedes a criminal investigation.

State entities subject to Section 208 of the State Technology Law that experience breaches of computerized data which includes private information must file notices with the New York Attorney General; Department of State's Division of Consumer Protection; and the Office of Information Technology Services' Enterprise Information Security Office.

Section 899-aa of the General Business Law provides that persons or businesses conducting business in New York must disclose any breaches of computerized data which includes private information by notifying the offices of the New York Attorney General; the NYS Division of State Police; and the Department of State's Division of Consumer Protection.

Information relative to the law and the notification process is available at: <http://www.dhses.ny.gov/ocs/breach-notification/>

5.24 Indemnification of New York State and Authorized Users for Breach of Security

The Contractor will indemnify DCJS and the State *without limitation* against any claims brought against DCJS and/or the State by reason of a wrongful disclosure of confidential information attributed to the Contractor or any of its agents, employees, and/or

subcontractors and will cooperate fully with DCJS, the State, and the Attorney General in defense of any claim(s).

The New York State General Business Law § 899-aa provides in part that:

6. (a) whenever the Attorney General shall believe from evidence satisfactory to him/her that there is a violation of this article he/she may bring an action in the name and on behalf of the people of the state of New York, in a court of justice having jurisdiction to issue an injunction, to enjoin and restrain the continuation of such violation. In such action, preliminary relief may be granted under article sixty-three of the civil practice law and rules. In such action the court may award damages for actual costs or losses incurred by a person entitled to notice pursuant to this article, if notification was not provided to such person pursuant to this article, including consequential financial losses. Whenever the court shall determine in such action that a person or business violated this article knowingly or recklessly, the court may impose a civil penalty of the greater of five thousand dollars or up to ten dollars per instance of failed notification, provided that the latter amount shall not exceed one hundred fifty thousand dollars.

The remedies in Section 6(a) are in addition to any other lawful remedy and in addition to any other remedy available under the terms of the Contract executed between The State and the Contractor.

The Contract executed between the State and the Contractor may be terminated by the State for cause for a material breach of this section, and the provisions of The New York State General Business Law § 899-aa shall survive the termination of this Agreement.

5.25 Nondisclosure & Confidentiality

The following shall supplement the requirements of Appendix B, General Specifications, paragraph 14 and Section 5.14.(D). Except as may be required by applicable law or a court of competent jurisdiction, the Contractor, its officers, agents, employees, and subcontractors, if any, shall maintain strict confidence with respect to any Confidential Information to which the Contractor, its officers, agents, employees, and subcontractors, if any, have access. The terms of this section shall survive termination or expiration of this Contract. Contractor agrees that its officers, agents, employees, and subcontractors, if any, performing Services for the State under this Contract shall be made aware of and shall agree in writing to the terms of this section. For purposes of this Contract, all State or Authorized Users information of which Contractor, its officers, agents, employees, and subcontractors, if any, becomes aware during the course of performing Services for the State shall be deemed to be confidential Information (oral, visual or written).

All information will be accounted for by the Contractor upon receipt and properly stored before, during, and after processing. In addition, all related output will be given the same level of protection as required for the source material.

The Contractor agrees that the data processed during the performance of the Contract will be completely purged from all data storage components of the Contractor's computer facility and no output will be retained by the Contractor at the time the work is completed, except for the documents required to be maintained pursuant to Section 5.7 and Appendix A paragraph 10. If immediate purging of all data storage components is not possible, the Contractor will certify that any data remaining in any storage component will be safeguarded to prevent unauthorized disclosures.

The Contractor will be responsible for the destruction of any intermediate hard copy printouts and will provide the NYS Project Manager, his/her designee, or any other named State employee or his/her designee with a statement containing the date of the destruction, description of material destroyed, and the method used. In the event that it becomes necessary for the Contractor to receive confidential information, which Federal or State statute or regulation prohibits from disclosure, the Contractor hereby agrees to return or destroy all such confidential information that has been received from the State when the purpose that necessitated its receipt by the Contractor has been completed. In addition, Contractor agrees not to retain any confidential information which Federal or State statute or regulation prohibits from disclosure after termination of the Contract.

Notwithstanding the foregoing, if the return or destruction of the confidential information is not feasible, the Contractor agrees to extend the protections of the Contract for as long as necessary to protect the confidential information and to limit any further use or disclosure of that confidential information by the Contractor. If Contractor elects to destroy confidential information, it shall use reasonable efforts to achieve the same and notify the State accordingly. The Contractor agrees that it will use all appropriate safeguards to prevent any unauthorized use or unauthorized disclosure of the State's confidential information, which Federal or State statute or regulation prohibits from disclosure.

The Contractor shall never disclose information which Federal, State statute, or regulation prohibits from disclosure.

The Contractor agrees that it shall immediately report to the State the discovery of any unauthorized use or unauthorized disclosure of such confidential information of any New York State agency or other Authorized User information directly to that New York State agency or other Authorized User.

Contractor shall hold the State harmless from any loss or damage to the State resulting from the disclosure by the Contractor, its officers, agents, employees, and subcontractors of such Confidential Information.

The State will have the right to terminate the Contract for cause if the Contractor fails to provide the safeguards described above or it is determined that the Contractor has violated a material term of this section.

Notwithstanding the language contained in this section, the Contractor may release any information pursuant to a final order issued from a Court of competent jurisdiction, provided the State has had an opportunity to be heard by such Court.

Notwithstanding the foregoing, information which falls into any of the following categories shall not be considered confidential information:

- a. Information that is previously rightfully known to the receiving party and accessible without restriction on disclosure;
- b. Information that becomes, from no act or failure to act on the part of the receiving party, generally known in the relevant industry or is in the public domain;
- c. Information that is independently developed by the Contractor without use of confidential information of the State;
- d. Information unrelated to the scope of this engagement; and
- e. That the State has approved for disclosure, but solely in accordance with the State's approval or direction.

5.26 Security

The following shall supplement the requirements of Appendix B paragraph 69. Contractor warrants, covenants and represents that it shall comply fully with all security procedures and policies of the State during the performance of the Contract. Contractor shall hold the State harmless from any loss or damage to the State resulting from the violation by the Contractor, its officers, agents, employees, and subcontractors, if any of such security procedures or policies resulting from any criminal acts committed by such officers, agents, employees, and subcontractors, while providing Services under the Contract.

The specific security procedures the Contractor shall implement include, but are not limited to:

- A. Data Access and Location– the Contractor must ensure that all data related to this project is stored in a controlled access environment to ensure data security and integrity. All access to State data, physical or virtual, must be conducted within the Continental United States and have adequate security systems in place to protect against the unauthorized access to the facilities and data stored therein. Adequate security systems must be in place to control access into

the facilities. The Contractor shall not send or permit to be sent to any location outside of the Continental United States any data related to this project. Access into and within the facilities must be restricted through an access control system that requires positive identification of authorized individuals as well as maintains a log of all accesses (e.g., date, time, who). The Contractor shall have a formal procedure in place for granting computer system access to the data and to track access. Access for projects outside of those approved by the State or an Authorized User is prohibited.

- B. Data Transport – The Contractor shall use reputable means to transport data. Deliveries must be made either via hand delivery by an employee of the Contractor or by restricted delivery via courier (e.g., FedEx, United Parcel Service, United States Postal Service) with shipment tracking and receipt confirmation. This applies to transport between the Contractor's offices, to and from subcontractors, and to the State.
- C. Data Protection – The Contractor shall use appropriate means to preserve and protect data related to this project. This includes, but is not limited to, use of stable storage media, regular data backups and archiving, password protection of volumes, and data encryption. The Contractor shall encrypt data identified by the State and using encryption methods approved by the State.
- D. Data Wiping – At the termination of the Contract, the Contractor will be required to wipe all data storage devices to eliminate any and all State data either collected or generated by the Contractor or provided by the State except for the documents required to be maintained pursuant to Appendix A paragraph 10. The wiping process must meet requirements set by the State.
- E. Data Breach Notification – Contractor agrees that it shall immediately report to the State the discovery of any unauthorized use or unauthorized disclosure of such Confidential Information of any New York State agency information directly to that New York State agency.
- G. Security Audits - Contractors may be asked to provide a recent independent audit report on security controls prior to formal awarding of any contract resulting from this RFP or at any time during the Contract term. The State and any regulatory authority having jurisdiction over the State or Authorized Users shall have the right to send its officers and employees into the offices and plants of the Contractor for inspection of the facilities and operations used in the performance of any work under the resulting Contract. On the basis of such inspection, specific measures may be required in cases where the Contractor is found to be noncompliant with Contract safeguards.

5.27 Criminal Justice Information Services (CJIS)

This RFP and its resulting Contract are strictly limited to permitting the Contractor to perform the services as described in the RFP and its resulting Contract. At no time shall the Contractor have access to any criminal history record information or other sensitive criminal justice information contained on Authorized Users Systems or media without complying with this section. Any access to computer media/systems which contain criminal history record information and other sensitive criminal justice information is subject to the Federal Bureau of Investigation Criminal Justice Information Services (CJIS) Security Policy, specifically the Security Addendum (SA) (annexed hereto as Appendix D). The purpose of the SA is to provide adequate security for criminal justice systems and information while under the management or control of a private entity or contractor. The SA strictly limits the authorized access to criminal history record information, limits the use of the information to the specific purposes for which it is being provided, ensures the security and confidentiality of the information consistent with applicable laws and regulations, provides for sanctions, and contains such other provisions as required by the FBI Director. Upon selection, the selected bidder and as a condition precedent for providing Project Services for the benefit of the Authorized Users, and as evidenced by the Successful Bidder signing the Contract, the Successful Bidder agrees (1) to abide by the SA, and (2) to the incorporation by reference of the SA as a part of the Contract, (3) that the SA shall be incorporated by reference as a part of all subcontract entered into by the Successful Bidder the purpose of which is of the delivery of Project Services, if any; and (4) that those Successful Bidder employees and subcontractor employees, if any that provide Project Services shall sign the form entitled, "Federal Bureau of Investigation Criminal Justice Information Services Security Addendum Certification" as set forth in RFP, Attachment 22. One copy of the signed form will be retained by the Successful Bidder and the original will be provided to the State for retention by the CJIS Information Security Officer for New York State.

5.28 NYS Cyber Security Policy P03-002

A. All information concerning NYS' operations, procedures and policies shall be kept confidential by the Contractor and the Contractor shall comply with administrative procedures and regulations concerning these rules. The Contractor shall take all steps required by NYS to protect confidential information. This will include fingerprint and background checks of Contractor personnel or any Contractor's subcontractor with access to such information and a requirement that the Contractor replace personnel or any such subcontractor at the discretion of the State.

B. Contractor must abide by the conditions set forth in the Appendix O, Cyber-Security-Policy-P03-002-V3.4 c. As a result of the security issues associated with the services to be performed by the Contractor, the Contractor and any associates and/or subcontractors will be required to insure that all work is performed within the continental United States.

5.29 User Data is the Property of New York State

In the course of performance of its obligations pursuant to this RFP and any resulting Contract the Contractor, its personnel, agents, officers, and any subcontractors may have access to or come into possession of data and information which is the property of DCJS or the State and data and information which is processed by or stored within DCJS or another State agency for the benefit of other entities. Such data includes but is not limited to fingerprint cards, criminal history information, employee and license application information, biometric identifiers, social security numbers, personally identifying information, photographs, palm prints and other data and information stored in electronic, optical or physical form including data and information concerning individuals and data and information concerning operations, processes, procedures and policies of NYS and other governmental entities.

All information concerning such aforementioned State operations, procedures and policies shall be kept confidential by the Contractor, its personnel, agents, officers, and any subcontractors, and the Contractor shall ensure that it and any such individuals or entities comply with DCJS and/or other State of New York administrative procedures and regulations concerning this requirement and take all steps required by DCJS and the State of New York to protect confidential information. This may include, but is not limited to, execution of non-disclosure agreements by Contractor's personnel, agents, and officers and the employees of any such subcontractors. If applicable to the environment, fingerprint checks and New York State Police background checks of the Contractor's personnel, agents, and officers and the employees of any subcontractors with access to such information in connection with the project, and a requirement that any Contractor's personnel, agents, and officers and the employees of any subcontractor must be approved by NYS. The Contractor shall be responsible for assuring NYS that it has notified all such individuals involved with the contract of the provisions of this section, and the Contractor shall require compliance with the provisions of this Section by performing or providing services to the Contractor in connection with this RFP and the resulting Contract.

The use of information obtained by such aforementioned Contractor and/or subcontractor individuals in the performance of its duties under this Agreement shall be limited to purposes directly connected with such duties with the understanding that none acquire any ownership, right to use, title or any interest in any data or information which remains the property of NYS or the property of the entities for which NYS is processing or storing the data or information.

The Contractor shall take appropriate precautions to ensure that Contractor's personnel, agents, and officers and the employees of any of its subcontractors;(i) shall never remove any work papers or product from the DCJS or any other State premises except with the written consent of DCJS or another designated State entity and(ii) never disclose, sell, publish, archive, make available in any form or summary any information of any kind

obtained in connection with performance under this RFP and any resulting Contract. The provisions of this section shall survive the termination of this Agreement.

5.30 Accounting/Audit

A. Maintenance of Supporting Documentation

The Contractor shall maintain all documentation supporting costs charged to the project, which shall be maintained for a minimum of seven (7) years beyond the Contract termination or any Contract amendment termination date.

B. Access to & Audit of Agreement Records

At all times during the contractual term and for a period of seven (7) years thereafter, the Contractor shall provide the NYS Comptroller, the Attorney General, and any other person or entity authorized to conduct an examination, as well as any other agencies or entities involved in this contract, with full access to the supporting documentation that pertains to services performed and determination of amounts payable under the Contract. Access shall be granted within five (5) business days. The Contractor will also make the appropriate individuals with knowledge of the supporting documentation of financial records related to the Contract (including the Contractor's independent public auditors) available to State representatives to answer questions and provide additional documentation where necessary. State representatives shall be permitted to examine, audit and copy such records at the site at which they are located. The Contractor shall be responsible for assuring that the provisions of this Section shall apply to any subcontract related to performance under the Contract.

5.31 Minority & Women Owned Business Enterprises

NEW YORK STATE LAW

Pursuant to New York State Executive Law Article 15-A, DCJS recognizes its obligation under the law to promote opportunities for maximum feasible participation of certified minority-and women-owned business enterprises and the employment of minority group members and women in the performance of DCJS contracts.

In 2006, the State of New York commissioned a disparity study to evaluate whether minority and women-owned business enterprises had a full and fair opportunity to participate in state contracting. The findings of the study were published on April 29, 2010, under the title "The State of Minority and Women-Owned Business Enterprises: Evidence from New York" ("Disparity Study"). The report found evidence of statistically significant disparities between the level of participation of minority-and women-owned business enterprises in state procurement contracting versus the number of minority-and women-owned business enterprises that were ready, willing and able to

participate in state procurements. As a result of these findings, the Disparity Study made recommendations concerning the implementation and operation of the statewide certified minority- and women-owned business enterprises program. The recommendations from the Disparity Study culminated in the enactment and the implementation of New York State Executive Law Article 15-A, which requires, among other things, that DCJS establishes goals for maximum feasible participation of New York State Certified minority- and women – owned business enterprises (“MWBE”) and the employment of minority groups members and women in the performance of New York State contracts.

Business Participation Opportunities for MWBEs

For purposes of this solicitation, DCJS hereby establishes an overall goal of 20% for MWBE participation, 15% for Minority-Owned Business Enterprises (“MBE”) participation and 5% for Women-Owned Business Enterprises (“WBE”) participation (based on the current availability of qualified MBEs and WBEs). A contractor (“Contractor”) on the subject contract (“Contract”) must document good faith efforts to provide meaningful participation by MWBEs as subcontractors or suppliers in the performance of the Contract and Contractor agrees that DCJS may withhold payment pending receipt of the required MWBE documentation. The directory of New York State Certified MWBEs can be viewed at: <http://www.esd.ny.gov/mwbe.html>. For guidance on how DCJS will determine a Contractor’s “good faith efforts,” refer to 5 NYCRR §142.8.

In accordance with 5 NYCRR §142.13, Contractor acknowledges that if it is found to have willfully and intentionally failed to comply with the MWBE participation goals set forth in the Contract, such finding constitutes a breach of Contract and DCJS may withhold payment from the Contractor as liquidated damages.

Such liquidated damages shall be calculated as an amount equaling the difference between: (1) all sums identified for payment to MWBEs had the Contractor achieved the contractual MWBE goals; and (2) all sums actually paid to MWBEs for work performed or materials supplied under the Contract.

By submitting a bid or proposal, a bidder on the Contract (“Bidder/”) agrees to submit the following documents and information as evidence of compliance with the foregoing:

- A. Bidders are required to submit a MWBE Utilization Plan with their bid or proposal. Any modifications or changes to the MWBE Utilization Plan after the Contract award and during the term of the Contract must be reported on a revised MWBE Utilization Plan and submitted to DCJS.
- B. DCJS will review the submitted MWBE Utilization Plan and advise the Bidder of DCJS acceptance or issue a notice of deficiency within 30 days of receipt.

- C. If a notice of deficiency is issued, Bidder agrees that it shall respond to the notice of deficiency within seven (7) business days of receipt by submitting to the DCJS a written remedy in response to the notice of deficiency. If the written remedy that is submitted is not timely or is found by [DCJS to be inadequate, DCJS shall notify the Bidder and direct the Bidder to submit, within five (5) business days, a request for a partial or total waiver of MWBE participation goals. Failure to file the waiver form in a timely manner may be grounds for disqualification of the bid or proposal.
- D. DCJS may disqualify a Bidder as being non-responsive under the following circumstances:
 - a) If a Bidder fails to submit a MWBE Utilization Plan;
 - b) If a Bidder fails to submit a written remedy to a notice of deficiency;
 - c) If a Bidder fails to submit a request for waiver; or
 - d) If DCJS determines that the Bidder has failed to document good faith efforts.

Contractors shall attempt to utilize, in good faith, any MBE or WBE identified within its MWBE Utilization Plan, during the performance of the Contract. Requests for a partial or total waiver of established goal requirements made subsequent to Contract Award may be made at any time during the term of the Contract to [DCJS but must be made no later than prior to the submission of a request for final payment on the Contract.

Contractors are required to submit a Contractor's Quarterly M/WBE Contractor Compliance & Payment Report DCJS by the 10th day following each end of quarter over the term of the Contract documenting the progress made toward achievement of the MWBE goals of the Contract.

Equal Employment Opportunity Requirements

By submission of a bid or proposal in response to this solicitation, the Bidder/Contractor agrees with all of the terms and conditions of Appendix A including Clause 12 - Equal Employment Opportunities for Minorities and Women. The Contractor is required to ensure that it and any subcontractors awarded a subcontract over \$25,000 for the construction, demolition, replacement, major repair, renovation, planning or design of real property and improvements thereon (the "Work") except where the Work is for the beneficial use of the Contractor, shall undertake or continue programs to ensure that minority group members and women are afforded equal employment opportunities without discrimination because of race, creed, color, national origin, sex, age, disability or marital status. For these purposes, equal opportunity shall apply in the areas of recruitment, employment, job assignment, promotion, upgrading, demotion, transfer, layoff, termination, and rates of pay or other forms of compensation. This requirement does not apply to: (i) work, goods, or services unrelated to the Contract; or (ii) employment outside New York State.

Bidder further agrees, where applicable, to submit with the bid a staffing plan (identifying the anticipated work force to be utilized on the Contract and if awarded a Contract, will, quarterly, submit to the DCJS , a workforce utilization report identifying the workforce actually utilized on the Contract if known.

Further, pursuant to Article 15 of the Executive Law (the “Human Rights Law”), all other State and Federal statutory and constitutional non-discrimination provisions, the Contractor and sub-contractors will not discriminate against any employee or applicant for employment because of race, creed (religion), color, sex, national origin, sexual orientation, military status, age, disability, predisposing genetic characteristic, marital status or domestic violence victim status, and shall also follow the requirements of the Human Rights Law with regard to non-discrimination on the basis of prior criminal conviction and prior arrest.

Please Note: Failure to comply with the foregoing requirements may result in a finding of non-responsiveness, non-responsibility and/or a breach of the Contract, leading to the withholding of funds, suspension or termination of the Contract or such other actions or enforcement proceedings as allowed by the Contract.

5.32 Payment of Outstanding Tax Liabilities

All outstanding tax liabilities if any, against the Contractor in favor of the State of New York must be satisfied prior to Contract execution or a payment schedule acceptable to the State of New York arranged for their speedy satisfaction.

5.33 Integration, Merger & Order of Precedence

The Agreement, including all appendices, attachments and exhibits, copies of which are attached and incorporated by reference, constitutes the entire Contract between the Parties. All prior agreements, representations, statements, negotiations and undertakings are superseded. All statements made by the State shall be deemed to be representations and not warranties. The Agreement is subject to amendment(s) only upon mutual consent of the Parties, reduced to writing and approved by the Office of the State Comptroller of the State of New York, where applicable.

This bid and any Contract shall incorporate the following appendices as if set forth herein at length. Only documents expressly enumerated below shall be deemed a part of this bid or Contract, and references contained in those documents to additional Contractor documents not enumerated below shall be of no force and effect. Conflicts between this solicitation, the Contractor’s proposal and Contract documents (if applicable) shall be resolved in the following order of precedence:

- 1) Appendix A (Standard Clauses for NYS Contracts). The parties agree that this contract is governed by and incorporates all of the terms and conditions of the

document identified as Appendix A – Standard Clauses for New York State Contracts dated January 2014 annexed hereto and which is incorporated into this Contract as though fully set forth in its entirety herein.

- 2) This Agreement;
- 3) The following Appendices and/or other attachments annexed to this Agreement:
 - The Public Safety Credentialing and Training System (PSCTS) Request For Proposals (RFP), dated _____, 2014, including all RFP appendices and attachments
 - Contractor's RFP Submission and all Attachments and Contractor's Clarification (where applicable), including any supporting material.
 - OSC Consultant Contractor Services Form A and Form B Addendum
 - MacBride Fair Employment – Northern Ireland Non-Discrimination
 - Non Collusive Bidding Certification (State Finance Law Section 139-d)
 - DCJS Procurement Lobbying Guidelines
 - State Finance Law Sections 139-j and 139-k Affirmation
 - Affirmation of Understanding and Agreement pursuant to State Finance Law §139-j (3) and §139-j (6) (b)
 - Disclosure of Prior Non Responsibility Determination
 - Workers Compensation coverage certificate
 - Proof of Disability Benefits Insurance OR Form CE-200 from Workers Compensation demonstrating relief from Workers Compensation/Disability (see www.wcb.ny.gov)
 - Minority and Women-Owned Business Enterprise (MWBE) and Equal Opportunities Requirements.
 - Any Change Request Order Form which is subsequently mutually entered into with respect to services during the terms of this Agreement;
 - Any Statement of Work (SOW) issued by NYS to the Contractor under the terms of this Agreement from time to time

The terms, provisions, representations and warranties contained in the Contract will survive performance hereunder.

5.34 Dispute Resolution and Escalation

In addition to any escalation procedure or problem resolution procedure established in connection with the delivery of specific Deliverables or Services under this Agreement, NYS and the Contractor shall have recourse to the dispute resolution procedure described herein. NYS staff and Contractor staff shall, in good faith and in a timely manner, attempt to resolve all disputes arising under this Agreement. NYS and the Contractor agree to the use of the following procedures should a dispute arise concerning their rights and responsibilities under this Agreement:

A. The NYS Project Manager and Contractor's Project Manager will be given the first opportunity to solve the dispute.

B. If the Project Managers cannot resolve the dispute within five (5) business days from the date on which the dispute arose, they will refer the dispute, in writing, to the ITS, Public Safety Cluster CIO or designee and the Contractor's signatory or designee. The memo will contain a description of the disputed issue and the date of event causing the dispute.

C. Contractor shall, in conjunction with the reporting requirements set forth herein, provide NYS with a written report quarterly of those disputes requiring action under paragraph B, above. Such report shall include an explanation of how each such dispute was resolved.

D. The foregoing dispute resolution procedure, or any determination or equitable allocation of costs included therein, shall not be deemed to limit either Party's rights or remedies under this Agreement.

5.35 Additional Responsibilities of the Contractor

A. If the Contractor's proposal includes goods or services provided by another firm, the Contractor shall assume full responsibility for the delivery, installation, maintenance and support services of such items offered in the proposal. The State will contract only with the Contractor. The State shall consider the Contractor to be the sole contact with regard to all provisions of the Contract.

B. The Contractor is responsible for meeting all obligations set forth in this RFP and any resulting Contract, including all exhibits, appendices and addenda, and any subsequent amendments mutually agreed to in writing between the parties. The Contractor acknowledges that the Contract is being entered into by the State in reliance on Contractor's representations concerning the particular qualifications, expertise, experience, financial standing and resources, management expertise and technical expertise of the Contractor and its staff assigned to provide Services under the Contract.

C. Throughout the Contract term, in addition to the requirements of the State Finance Law § 138 (requiring the State's approval of subcontractors), in the event that there is a substantial or material change, as defined below, in the ownership or financial viability of the Contractor, its corporate affiliates, subsidiaries, or divisions, the Contractor is required to provide notice and details of any such change to the State in writing immediately when such is first known by Contractor, its corporate affiliates, subsidiaries or divisions, or subcontractors. "Substantial" or "material" change shall be defined to include, but not be limited to; sale, acquisitions, mergers, or takeovers involving the Contractor, its corporate affiliates, subsidiaries or divisions, or partners that result in a change in the controlling ownership or assets of such entity after the submission of the Proposal; or entry of an order for relief under Title 11 of the United States Code; the

making of a general assignment for the benefit of creditors; the appointment of a general receiver or trustee in bankruptcy of Contractor's, its corporate affiliates, subsidiaries or divisions, or partners' business or property; or action by Contractor, its corporate affiliates, subsidiaries or divisions, or partners under any state insolvency or similar law for the purposes of its bankruptcy, reorganization or liquidation; or court ordered liquidation against Contractor, its corporate affiliates, subsidiaries or divisions, or partners. Upon the State's receipt of such notice, the State shall have thirty (30) business days from the date of notice to review the information. The Contractor may not transfer the Contract among corporate affiliates, subsidiaries or divisions, or partners without the written consent of the State. In addition to any other remedies available at law or equity, the State shall have the right to prospectively cancel the Contract, in whole or in part, for cause if it finds that such change materially and adversely affects the delivery of Services solely determined with reference to the best interests of the State.

D. The Contractor shall acquire the prior written approval of the State before it assigns its right to receive payment under the Contract.

E. The Contractor shall notify the State in writing of any changes in the person or persons authorized to sign amendments to the Contract on behalf of the Contractor.

F. The Contractor shall assume sole and complete responsibility for the cost and timely completion of all activities required under this RFP and any resulting Contract.

G. The Contractor shall fully cooperate with any other contractors, such as hardware providers, that may be engaged by the State or User to work on the project.

H. The Contractor shall disclose the names and addresses of those subcontractors whose products or services materially contribute to the product or service procured from the Contractor (see Attachments 18 and 19). The Contractor must guarantee the work of subcontractors as if it were its own.

I. Provide a full-time Project Manager dedicated to the PSCTS project. The Project Manager must be fluent in the English language (e.g., listens, speaks, reads, writes, understands, and comprehends English fluently). This manager will be responsible for directing the work of the Contractor resources, coordinating and communicating with the NYS Project Manager and ensuring the project deliverables are met according to the Project Plan.

J. Provide an Account Manager dedicated to the NYS account. The Account Manager must be fluent in the English language (e.g., listens, speaks, reads, writes, understands, and comprehends English fluently). This manager, separate from the Project Manager, will be responsible for directly interfacing with the Stakeholders of the PSCTS project.

K. Maintain the continuity of the Contractor team staffing throughout the course of the implementation phase of the project. NYS reserves the right to approve/disapprove

changes in Contractor resources. Replacement resources must have comparable or better skills.

L. All documentation offered to the Contractor firms to assist in their efforts will be turned over to the New York State when their work has been completed. Any documentation created as part of any assignment is the property of NYS and will be turned over to NYS in paper and/or electronic format at the discretion of NYS.

5.36 New York State Responsibilities

Initially, the New York State Division of Criminal Justice Services (DCJS) will assign a resource to act as the liaison for the agency and as a primary contact for the Contractor. The DCJS contact will answer all technical and analytical questions for the Contractor. Subsequently, another authorized State agency may assign a designated person for such purposes.

5.37 Extension of Existing Product Line – New Products

A. Until the date of acceptance testing, if technological improvements have been made to the products available for purchase under this Contract, the Contractor may propose new products that are an extension of an existing product line or the “next generation” of an existing product line that meet or exceed the specification(s) of existing products under this Contract, if the price for the new product does not exceed:

- i. The ceiling price for the product originally offered in the Contractor’s proposal;
- ii. The current published list price of the replacement product, less any applicable Government discount; or
- iii. The price at which the replacement product is generally available for purchase, whichever is lowest.

B. The proposed new product may be subject to benchmark evaluation and all costs associated with the benchmark evaluation (e.g., transportation, benchmark fee, etc.) shall be at the Contractor’s expense.

C. Whether or not to accept or reject a proposed new product is entirely within the discretion of NYS. If NYS does not accept a proposed new product, the Contractor shall continue to be obligated to deliver the original product.

D. If accepted, the addition of the new product will be documented for the administrative purposes of NYS by a contract amendment, by adding the new product to this Contract.

5.38 Partial Invalidity

In the event that any provision of a resulting Contract is declared or found to be illegal, unenforceable, ineffective or void, then each party shall be relieved of any obligation

arising from such provision. The balance of the Contract shall remain in full force and effect, if capable of performance.

5.39 Not Employees of the State

The State and the Contractor agree that the Contractor is an independent contractor, and the Contractor, its agents, officers and employees, in the performance of this Agreement, shall act in an independent capacity and not as officers or employees of the State.

5.40 Waiver

No term or provision of the Agreement shall be deemed waived and no breach excused, unless such waiver or consent shall be in writing and signed by the Party claimed to have waived or consented. No consent by a Party to, or waiver of, a breach under the Agreement shall constitute consent to, a waiver of, or excuse for any other, different or subsequent breach. The rights, duties and remedies set forth in the Agreement shall be in addition to, and not in limitation of, rights and obligations otherwise available at law or equity.

5.41 Taxes

Except as otherwise provided by applicable Federal and State law and regulations, the State shall not be liable for the payment of any taxes under the Contract, however they are designated, levied, or imposed. Purchases made by the State are exempt from New York State local sales and use taxes and, with certain exceptions, from Federal excise taxes. To satisfy the requirements of the New York State Sales and Use Tax Law, invoices issued by the Contractor pursuant to the Contract shall reference the Contract in order to be considered sufficient evidence that the sale by Contractor was made to the State. The State is an exempt organization under Section 1116(a)(1) of the Tax Law. However, no person, firm, or corporation is exempt from paying the State Truck Mileage and Unemployment Insurance taxes and other Federal, State and local taxes to which Contractor is subject. The New York State Registration Number for the purpose of tax free transactions under the Internal Revenue Code shall be provided to the Contractor by NYS. Nothing in this section shall be construed to limit the obligation of the State to reimburse Contractor for approved expenses, including valid State and local taxes, under the Contract. Sales tax registration and certification requirements must be met and documentation must be provided to NYS by the Contractor.

5.42 Extraneous Terms

New York State law prohibits the State from awarding a contract based upon material deviations from the specifications, terms, and conditions set forth in this RFP. Therefore, extraneous terms and conditions are proposed solely at the Bidder's risk as they may be deemed material deviations by the State and may render the Proposal non-responsive,

resulting in its rejection. Proposed additional, supplemental, “or equal,” or alternative terms (Extraneous Term(s)) may only be considered by the State to the extent that such Extraneous Term(s) constitute non-material deviations from the requirements set forth in the RFP. If the Bidder proposes to include Extraneous Terms in its official Proposal, the Bidder shall meet all of the following requirements:

- A. Each proposed Extraneous Term shall be specifically enumerated in a separate section of the applicable submission (Administrative, Technical, or Financial) labeled “Additional/Extraneous Terms”; and;
- B. The “Extraneous Terms” section shall be prepared by the Bidder and may not include any pre-printed literature or vendor forms;
- C. The writing shall identify by part, section, and title the particular RFP requirement (if any) affected by the Extraneous Term; and;
- D. The Bidder shall specify the proposed Extraneous Term and the reasons therefore.

Only those terms meeting the above requirements (A) through (D) shall be considered as having been submitted as part of the formal offer. Extraneous Term(s) submitted on standard, pre-printed forms (including, but not limited to: product literature, order forms, manufacturer’s license agreements, standard contracts, or other preprinted documents) that are physically attached or summarily referenced in the Proposal, or that, in the State’s sole judgment, have not been submitted in compliance with the above requirements (A) through (D), will not be considered as having been submitted with or intended to be incorporated as part of the official offer contained in the Proposal, but rather will be deemed by the State to have been included by Bidder for informational or promotional purposes only.

Absent the State’s express written acceptance and incorporation of an Extraneous Term, acceptance and/or processing of the Proposal shall not constitute the State’s acceptance of Extraneous Term(s) or be deemed a waiver of the State’s rights set forth in this section.

5.43 Severability

In the event that one or more of the provisions of the Contract shall for any reason be declared unenforceable by a court of competent jurisdiction under the laws or regulations in force, such provision(s) shall have no effect on the validity of the remainder of the Contract, which shall then be construed as if such unenforceable provision was never contained in the Contract.

5.44 Assignment of Claim

Contractor hereby assigns to the State any and all of its claims for overcharges associated with the Contract that may arise under the antitrust laws of the United States, 15 U.S.C.

Section 1, *et seq.* and the antitrust laws of the State of New York, General Business Law Section 340, *et seq.*

5.45 Notification

Any notice required by or pertaining to this Contract shall be delivered to the other Party in writing, by certified mail, return receipt requested, addressed to (unless otherwise specified in the Contract) the recipient Party's signatory to the Contract or his/her designee. The date of notice shall be deemed the date of delivery set forth on the return receipt (the "date of return receipt notice"). Such notice shall be addressed as follows:

Michael C. Green
Commissioner
State of New York
Division of Criminal Justice Services
Alfred E. Smith Office Building, 8th Floor
80 South Swan Street
Albany, NY 12210

With a copy to:

Gina L. Bianchi
Deputy Commissioner and Counsel
State of New York
Division of Criminal Justice Services
Office of Legal Services
Alfred E. Smith Office Building, 8th Floor
80 South Swan Street
Albany, NY 12210

Contractor:

_ INSERT NAME, TITLE, AND BUSINESS ADDRESS_____

5.46 Notice to State

The Contractor shall immediately notify the State upon learning of any situation that can reasonably be expected to adversely affect the delivery of Services under the Contract. If such notification is verbal, the Contractor shall submit to the State a written description

of the situation and a recommendation for its resolution within seven (7) business days of learning of the situation.

5.47 Suspension of Work

NYS reserves the right to suspend any or all activities under the Contract, at any time, in the best interests of the State or of DCJS. In the event of such suspension, the Contractor will be given a formal written notice outlining the particulars of such suspension. Examples of the reason for such suspension include, but are not limited to, a budget freeze on State spending, declaration of emergency, or other such circumstances. Upon issuance of such notice, the Contractor shall comply with the suspension order. Activity may resume at such time as NYS issues a formal written notice authorizing a resumption of work.

5.48 General Provision as to Remedies

The parties may exercise their respective rights and remedies at any time, in any order, to any extent, and as often as deemed advisable, without regard to whether the exercise of one right or remedy precedes, concurs with or succeeds the exercise of another. A single or partial exercise of a remedy shall not preclude a further exercise of the right or remedy or the exercise of another right or remedy from time to time. No delay or omission in exercising a right or remedy, or delay, inaction, or waiver of any event of default, shall exhaust or impair the right or remedy or constitute a waiver of, or acquiescence to, an event otherwise constituting a breach or default under this Contract.

In addition to any other remedies available to NYS under the Contract, NYS has additional remedies that may include, but are not limited to, the following:

- A. The right for NYS to withhold payment of some or all of the amounts due and owed under the Contract until Contractor's performance is brought within the specified parameters.
- B. The application of credits against amounts due and owed by NYS under the Contract.

5.49 Liquidated Damages

The existing PSCTS in operation at NYS has reached the end of its useful life. The existing system serves the PSCTS processing, database and search requirements of NYS and law enforcement agencies throughout New York State. The new PSCTS, which will enhance PSCTS information and incorporate existing PSCTS' database, will advance both public safety and programmatic accountability. Its failure or degradation will result in damages that are impossible to calculate. Damages include but are not limited to exposure of personal identifying information, loss of statutorily mandated retention

records, loss of information of an evidentiary nature and the possible exposure of individuals in sensitive and/or undercover positions which could put said individuals in imminent danger.

Because the current system has reached the end of its useful life, NYS is making provision for its replacement through this procurement and must ensure that the replacement PSCTS is timely completed, performs as specified, that the database conversion is executed with the required degree of accuracy and that the transition between the legacy system and the PSCTS replacement occurs on time and without incident.

Contractor's failure to deliver or install individual project deliverables within time frames agreed to by the parties or providing timely but unacceptable deliveries may cause incalculable damage to NYS and its law enforcement partners and to the citizens which will be impacted by such failure.

The Contractor must agree that in the event that it fails to deliver and install the PSCTS and complete acceptance testing by the date as specified in the contract or any amendment thereof the contract shall subject Contractor to liquidated damages as determined by the State which may be in the amount of one (1.00%) percent of the contract value of any late deliverable for each day that receipt is delayed over the stated time frame, up to the full amount of the contracted price of the PSCTS.

These liquidated damages are not a penalty, but shall be in lieu of certain other remedies and may be deducted from payments due or to become due and may be assessed against the Contractor's bond or insurance, where applicable. However, notwithstanding a determination to assess liquidated damages, NYS may elect to determine that a Contractor is in substantial breach of the contract and terminate the contract completely, and elect to sue for all damages which NYS has incurred; in such case the Contractor shall receive a credit for any liquidated damages it shall have paid prior to termination.

In the event that the Contractor has failed to deliver and install the PSCTS and complete acceptance testing by six months following the date on which the Comptroller approves the contract, NYS shall give the Contractor written notice of the intent to assess such damages and thirty (30) calendar days opportunity to cure before the liquidated amount will be assessed against the Contractor.

This provision shall not apply to the extent or for any periods where the NYS or a force majeure is the cause of such delay.

5.50 Extension of Use

Any contract resulting from this bid solicitation shall contain a provision that grants the option to allow additional State or governmental agencies to purchase from the Contractor under the terms and conditions of the contract. Political subdivisions and other

authorized entities within each participating State or governmental jurisdiction may also participate in any resultant contract if such State normally allows participation by such entities. New York State reserves the right to negotiate additional discounts based on any increased volume generated by such extensions.

5.51 Foreign Nationals

The Federal Immigration Reform and Control Act, as amended, (8 USC Section 1324a et al) obligates employers, such as the Contractors, to verify that all its employees are legally entitled to work in the United States. In order to verify that an individual is not an unauthorized alien, NYS reserve the right to request legally mandated Contractor help documentation attesting to the legal entitlement to work in the United States for each consultant assigned work under any contract awarded. In according with such law, NYS and its Authorized Users do not discriminate against individuals on the basis of national origin or citizenship.

5.52 Headings Have No Legal Significance

Headings, the Table of Contents and the Glossary included within this document have no legal or factual significance, are provided for the convenience of the reader and may not be otherwise relied on.

5.53 Penalties for Non Performance

This RFP sets forth the State's mandatory base system requirements for availability of the Proposed Solution which the Contractor is required to meet throughout the term of the Contract and applicable extensions. Failure to meet the requirements may result in penalties for non-performance in addition to any other available remedy available to the State under the terms of this RFP and resulting Contract. As, the Offerer is proposing a solution that meets the public safety requirements of the State and because the system is a public safety system which serves law enforcement, its failure or degradation may result in damages that are impossible to calculate. Additional pecuniary damages may result from NYS securing or attempting to secure replacement services for the period in which the Contractor fails to perform, although such alternatives are not capable of providing adequate cover and cannot completely mitigate the risk associated with the Contractor's failure to perform.

Appendix A

STANDARD CLAUSES FOR NEW YORK STATE CONTRACTS

PLEASE RETAIN THIS DOCUMENT
FOR FUTURE REFERENCE.

TABLE OF CONTENTS

	Page
1. Executory Clause	3
2. Non-Assignment Clause	3
3. Comptroller's Approval	3
4. Workers' Compensation Benefits	3
5. Non-Discrimination Requirements	3
6. Wage and Hours Provisions	3
7. Non-Collusive Bidding Certification	4
8. International Boycott Prohibition	4
9. Set-Off Rights	4
10. Records	4
11. Identifying Information and Privacy Notification	4
12. Equal Employment Opportunities For Minorities and Women	4-5
13. Conflicting Terms	5
14. Governing Law	5
15. Late Payment	5
16. No Arbitration	5
17. Service of Process	5
18. Prohibition on Purchase of Tropical Hardwoods	5-6
19. MacBride Fair Employment Principles	6
20. Omnibus Procurement Act of 1992	6
21. Reciprocity and Sanctions Provisions	6
22. Compliance with New York State Information Security Breach and Notification Act	6
23. Compliance with Consultant Disclosure Law	6
24. Procurement Lobbying	7
25. Certification of Registration to Collect Sales and Compensating Use Tax by Certain State Contractors, Affiliates and Subcontractors	7
26. Iran Divestment Act	7

STANDARD CLAUSES FOR NYS CONTRACTS

The parties to the attached contract, license, lease, amendment or other agreement of any kind (hereinafter, "the contract" or "this contract") agree to be bound by the following clauses which are hereby made a part of the contract (the word "Contractor" herein refers to any party other than the State, whether a contractor, licenser, licensee, lessor, lessee or any other party):

1. EXECUTORY CLAUSE. In accordance with Section 41 of the State Finance Law, the State shall have no liability under this contract to the Contractor or to anyone else beyond funds appropriated and available for this contract.

2. NON-ASSIGNMENT CLAUSE. In accordance with Section 138 of the State Finance Law, this contract may not be assigned by the Contractor or its right, title or interest therein assigned, transferred, conveyed, sublet or otherwise disposed of without the State's previous written consent, and attempts to do so are null and void. Notwithstanding the foregoing, such prior written consent of an assignment of a contract let pursuant to Article XI of the State Finance Law may be waived at the discretion of the contracting agency and with the concurrence of the State Comptroller where the original contract was subject to the State Comptroller's approval, where the assignment is due to a reorganization, merger or consolidation of the Contractor's business entity or enterprise. The State retains its right to approve an assignment and to require that any Contractor demonstrate its responsibility to do business with the State. The Contractor may, however, assign its right to receive payments without the State's prior written consent unless this contract concerns Certificates of Participation pursuant to Article 5-A of the State Finance Law.

3. COMPTROLLER'S APPROVAL. In accordance with Section 112 of the State Finance Law (or, if this contract is with the State University or City University of New York, Section 355 or Section 6218 of the Education Law), if this contract exceeds \$50,000 (or the minimum thresholds agreed to by the Office of the State Comptroller for certain S.U.N.Y. and C.U.N.Y. contracts), or if this is an amendment for any amount to a contract which, as so amended, exceeds said statutory amount, or if, by this contract, the State agrees to give something other than money when the value or reasonably estimated value of such consideration exceeds \$10,000, it shall not be valid, effective or binding upon the State until it has been approved by the State Comptroller and filed in his office. Comptroller's approval of contracts let by the Office of General Services is required when such contracts exceed \$85,000 (State Finance Law Section 163.6-a). However, such pre-approval shall not be required for any contract established as a centralized contract through the Office of General Services or for a purchase order or other transaction issued under such centralized contract.

4. WORKERS' COMPENSATION BENEFITS. In accordance with Section 142 of the State Finance Law, this January 2014

contract shall be void and of no force and effect unless the Contractor shall provide and maintain coverage during the life of this contract for the benefit of such employees as are required to be covered by the provisions of the Workers' Compensation Law.

5. NON-DISCRIMINATION REQUIREMENTS. To the extent required by Article 15 of the Executive Law (also known as the Human Rights Law) and all other State and Federal statutory and constitutional non-discrimination provisions, the Contractor will not discriminate against any employee or applicant for employment because of race, creed, color, sex (including gender identity or expression), national origin, sexual orientation, military status, age, disability, predisposing genetic characteristics, marital status or domestic violence victim status. Furthermore, in accordance with Section 220-e of the Labor Law, if this is a contract for the construction, alteration or repair of any public building or public work or for the manufacture, sale or distribution of materials, equipment or supplies, and to the extent that this contract shall be performed within the State of New York, Contractor agrees that neither it nor its subcontractors shall, by reason of race, creed, color, disability, sex, or national origin: (a) discriminate in hiring against any New York State citizen who is qualified and available to perform the work; or (b) discriminate against or intimidate any employee hired for the performance of work under this contract. If this is a building service contract as defined in Section 230 of the Labor Law, then, in accordance with Section 239 thereof, Contractor agrees that neither it nor its subcontractors shall by reason of race, creed, color, national origin, age, sex or disability: (a) discriminate in hiring against any New York State citizen who is qualified and available to perform the work; or (b) discriminate against or intimidate any employee hired for the performance of work under this contract. Contractor is subject to fines of \$50.00 per person per day for any violation of Section 220-e or Section 239 as well as possible termination of this contract and forfeiture of all moneys due hereunder for a second or subsequent violation.

6. WAGE AND HOURS PROVISIONS. If this is a public work contract covered by Article 8 of the Labor Law or a building service contract covered by Article 9 thereof, neither Contractor's employees nor the employees of its subcontractors may be required or permitted to work more than the number of hours or days stated in said statutes, except as otherwise provided in the Labor Law and as set forth in prevailing wage and supplement schedules issued by the State Labor Department. Furthermore, Contractor and its subcontractors must pay at least the prevailing wage rate and pay or provide the prevailing supplements, including the premium rates for overtime pay, as determined by the State Labor Department in accordance with the Labor Law. Additionally, effective April 28, 2008, if this is a public work contract covered by Article 8 of the Labor Law, the Contractor understands and agrees that the filing of payrolls in a manner consistent with Subdivision 3-a of Section 220 of the Labor Law shall be a condition precedent to payment by the State of

any State approved sums due and owing for work done upon the project.

7. NON-COLLUSIVE BIDDING CERTIFICATION. In accordance with Section 139-d of the State Finance Law, if this contract was awarded based upon the submission of bids, Contractor affirms, under penalty of perjury, that its bid was arrived at independently and without collusion aimed at restricting competition. Contractor further affirms that, at the time Contractor submitted its bid, an authorized and responsible person executed and delivered to the State a non-collusive bidding certification on Contractor's behalf.

8. INTERNATIONAL BOYCOTT PROHIBITION. In accordance with Section 220-f of the Labor Law and Section 139-h of the State Finance Law, if this contract exceeds \$5,000, the Contractor agrees, as a material condition of the contract, that neither the Contractor nor any substantially owned or affiliated person, firm, partnership or corporation has participated, is participating, or shall participate in an international boycott in violation of the federal Export Administration Act of 1979 (50 USC App. Sections 2401 et seq.) or regulations thereunder. If such Contractor, or any of the aforesaid affiliates of Contractor, is convicted or is otherwise found to have violated said laws or regulations upon the final determination of the United States Commerce Department or any other appropriate agency of the United States subsequent to the contract's execution, such contract, amendment or modification thereto shall be rendered forfeit and void. The Contractor shall so notify the State Comptroller within five (5) business days of such conviction, determination or disposition of appeal (2NYCRR 105.4).

9. SET-OFF RIGHTS. The State shall have all of its common law, equitable and statutory rights of set-off. These rights shall include, but not be limited to, the State's option to withhold for the purposes of set-off any moneys due to the Contractor under this contract up to any amounts due and owing to the State with regard to this contract, any other contract with any State department or agency, including any contract for a term commencing prior to the term of this contract, plus any amounts due and owing to the State for any other reason including, without limitation, tax delinquencies, fee delinquencies or monetary penalties relative thereto. The State shall exercise its set-off rights in accordance with normal State practices including, in cases of set-off pursuant to an audit, the finalization of such audit by the State agency, its representatives, or the State Comptroller.

10. RECORDS. The Contractor shall establish and maintain complete and accurate books, records, documents, accounts and other evidence directly pertinent to performance under this contract (hereinafter, collectively, "the Records"). The Records must be kept for the balance of the calendar year in which they were made and for six (6) additional years thereafter. The State Comptroller, the Attorney General and

any other person or entity authorized to conduct an examination, as well as the agency or agencies involved in this contract, shall have access to the Records during normal business hours at an office of the Contractor within the State of New York or, if no such office is available, at a mutually agreeable and reasonable venue within the State, for the term specified above for the purposes of inspection, auditing and copying. The State shall take reasonable steps to protect from public disclosure any of the Records which are exempt from disclosure under Section 87 of the Public Officers Law (the "Statute") provided that: (i) the Contractor shall timely inform an appropriate State official, in writing, that said records should not be disclosed; and (ii) said records shall be sufficiently identified; and (iii) designation of said records as exempt under the Statute is reasonable. Nothing contained herein shall diminish, or in any way adversely affect, the State's right to discovery in any pending or future litigation.

11. IDENTIFYING INFORMATION AND PRIVACY NOTIFICATION.

(a) Identification Number(s). Every invoice or New York State Claim for Payment submitted to a New York State agency by a payee, for payment for the sale of goods or services or for transactions (e.g., leases, easements, licenses, etc.) related to real or personal property must include the payee's identification number. The number is any or all of the following: (i) the payee's Federal employer identification number, (ii) the payee's Federal social security number, and/or (iii) the payee's Vendor Identification Number assigned by the Statewide Financial System. Failure to include such number or numbers may delay payment. Where the payee does not have such number or numbers, the payee, on its invoice or Claim for Payment, must give the reason or reasons why the payee does not have such number or numbers.

(b) Privacy Notification. (1) The authority to request the above personal information from a seller of goods or services or a lessor of real or personal property, and the authority to maintain such information, is found in Section 5 of the State Tax Law. Disclosure of this information by the seller or lessor to the State is mandatory. The principal purpose for which the information is collected is to enable the State to identify individuals, businesses and others who have been delinquent in filing tax returns or may have understated their tax liabilities and to generally identify persons affected by the taxes administered by the Commissioner of Taxation and Finance. The information will be used for tax administration purposes and for any other purpose authorized by law. (2) The personal information is requested by the purchasing unit of the agency contracting to purchase the goods or services or lease the real or personal property covered by this contract or lease. The information is maintained in the Statewide Financial System by the Vendor Management Unit within the Bureau of State Expenditures, Office of the State Comptroller, 110 State Street, Albany, New York 12236.

12. EQUAL EMPLOYMENT OPPORTUNITIES FOR MINORITIES AND WOMEN.

In accordance with Section 312 of the Executive Law and 5 NYCRR 143, if this contract is: (i) a written agreement or purchase order instrument, providing for a total expenditure in excess of \$25,000.00, whereby a contracting agency is committed to expend or does expend funds in return for labor, services, supplies, equipment, materials or any combination of the foregoing, to be performed for, or rendered or furnished to the contracting agency; or (ii) a written agreement in excess of \$100,000.00 whereby a contracting agency is committed to expend or does expend funds for the acquisition, construction, demolition, replacement, major repair or renovation of real property and improvements thereon; or (iii) a written agreement in excess of \$100,000.00 whereby the owner of a State assisted housing project is committed to expend or does expend funds for the acquisition, construction, demolition, replacement, major repair or renovation of real property and improvements thereon for such project, then the following shall apply and by signing this agreement the Contractor certifies and affirms that it is Contractor's equal employment opportunity policy that:

(a) The Contractor will not discriminate against employees or applicants for employment because of race, creed, color, national origin, sex, age, disability or marital status, shall make and document its conscientious and active efforts to employ and utilize minority group members and women in its work force on State contracts and will undertake or continue existing programs of affirmative action to ensure that minority group members and women are afforded equal employment opportunities without discrimination. Affirmative action shall mean recruitment, employment, job assignment, promotion, upgradings, demotion, transfer, layoff, or termination and rates of pay or other forms of compensation;

(b) at the request of the contracting agency, the Contractor shall request each employment agency, labor union, or authorized representative of workers with which it has a collective bargaining or other agreement or understanding, to furnish a written statement that such employment agency, labor union or representative will not discriminate on the basis of race, creed, color, national origin, sex, age, disability or marital status and that such union or representative will affirmatively cooperate in the implementation of the Contractor's obligations herein; and

(c) the Contractor shall state, in all solicitations or advertisements for employees, that, in the performance of the State contract, all qualified applicants will be afforded equal employment opportunities without discrimination because of race, creed, color, national origin, sex, age, disability or marital status.

Contractor will include the provisions of "a", "b", and "c" above, in every subcontract over \$25,000.00 for the construction, demolition, replacement, major repair, January 2014

renovation, planning or design of real property and improvements thereon (the "Work") except where the Work is for the beneficial use of the Contractor. Section 312 does not apply to: (i) work, goods or services unrelated to this contract; or (ii) employment outside New York State. The State shall consider compliance by a contractor or subcontractor with the requirements of any federal law concerning equal employment opportunity which effectuates the purpose of this section. The contracting agency shall determine whether the imposition of the requirements of the provisions hereof duplicate or conflict with any such federal law and if such duplication or conflict exists, the contracting agency shall waive the applicability of Section 312 to the extent of such duplication or conflict. Contractor will comply with all duly promulgated and lawful rules and regulations of the Department of Economic Development's Division of Minority and Women's Business Development pertaining hereto.

13. CONFLICTING TERMS. In the event of a conflict between the terms of the contract (including any and all attachments thereto and amendments thereof) and the terms of this Appendix A, the terms of this Appendix A shall control.

14. GOVERNING LAW. This contract shall be governed by the laws of the State of New York except where the Federal supremacy clause requires otherwise.

15. LATE PAYMENT. Timeliness of payment and any interest to be paid to Contractor for late payment shall be governed by Article 11-A of the State Finance Law to the extent required by law.

16. NO ARBITRATION. Disputes involving this contract, including the breach or alleged breach thereof, may not be submitted to binding arbitration (except where statutorily authorized), but must, instead, be heard in a court of competent jurisdiction of the State of New York.

17. SERVICE OF PROCESS. In addition to the methods of service allowed by the State Civil Practice Law & Rules ("CPLR"), Contractor hereby consents to service of process upon it by registered or certified mail, return receipt requested. Service hereunder shall be complete upon Contractor's actual receipt of process or upon the State's receipt of the return thereof by the United States Postal Service as refused or undeliverable. Contractor must promptly notify the State, in writing, of each and every change of address to which service of process can be made. Service by the State to the last known address shall be sufficient. Contractor will have thirty (30) calendar days after service hereunder is complete in which to respond.

18. PROHIBITION ON PURCHASE OF TROPICAL HARDWOODS. The Contractor certifies and warrants that all wood products to be used under this contract award will be in accordance with, but not limited to, the specifications and

provisions of Section 165 of the State Finance Law, (Use of Tropical Hardwoods) which prohibits purchase and use of tropical hardwoods, unless specifically exempted, by the State or any governmental agency or political subdivision or public benefit corporation. Qualification for an exemption under this law will be the responsibility of the contractor to establish to meet with the approval of the State.

In addition, when any portion of this contract involving the use of woods, whether supply or installation, is to be performed by any subcontractor, the prime Contractor will indicate and certify in the submitted bid proposal that the subcontractor has been informed and is in compliance with specifications and provisions regarding use of tropical hardwoods as detailed in §165 State Finance Law. Any such use must meet with the approval of the State; otherwise, the bid may not be considered responsive. Under bidder certifications, proof of qualification for exemption will be the responsibility of the Contractor to meet with the approval of the State.

19. MACBRIDE FAIR EMPLOYMENT PRINCIPLES.

In accordance with the MacBride Fair Employment Principles (Chapter 807 of the Laws of 1992), the Contractor hereby stipulates that the Contractor either (a) has no business operations in Northern Ireland, or (b) shall take lawful steps in good faith to conduct any business operations in Northern Ireland in accordance with the MacBride Fair Employment Principles (as described in Section 165 of the New York State Finance Law), and shall permit independent monitoring of compliance with such principles.

20. OMNIBUS PROCUREMENT ACT OF 1992. It is the policy of New York State to maximize opportunities for the participation of New York State business enterprises, including minority and women-owned business enterprises as bidders, subcontractors and suppliers on its procurement contracts.

Information on the availability of New York State subcontractors and suppliers is available from:

NYS Department of Economic Development
Division for Small Business
Albany, New York 12245
Telephone: 518-292-5100
Fax: 518-292-5884
email: opa@esd.ny.gov

A directory of certified minority and women-owned business enterprises is available from:

NYS Department of Economic Development
Division of Minority and Women's Business Development
633 Third Avenue
New York, NY 10017

212-803-2414

email: mwbecertification@esd.ny.gov

<https://ny.newnycontracts.com/FrontEnd/VendorSearchPublic.asp>

The Omnibus Procurement Act of 1992 requires that by signing this bid proposal or contract, as applicable, Contractors certify that whenever the total bid amount is greater than \$1 million:

(a) The Contractor has made reasonable efforts to encourage the participation of New York State Business Enterprises as suppliers and subcontractors, including certified minority and women-owned business enterprises, on this project, and has retained the documentation of these efforts to be provided upon request to the State;

(b) The Contractor has complied with the Federal Equal Opportunity Act of 1972 (P.L. 92-261), as amended;

(c) The Contractor agrees to make reasonable efforts to provide notification to New York State residents of employment opportunities on this project through listing any such positions with the Job Service Division of the New York State Department of Labor, or providing such notification in such manner as is consistent with existing collective bargaining contracts or agreements. The Contractor agrees to document these efforts and to provide said documentation to the State upon request; and

(d) The Contractor acknowledges notice that the State may seek to obtain offset credits from foreign countries as a result of this contract and agrees to cooperate with the State in these efforts.

21. RECIPROCITY AND SANCTIONS PROVISIONS.

Bidders are hereby notified that if their principal place of business is located in a country, nation, province, state or political subdivision that penalizes New York State vendors, and if the goods or services they offer will be substantially produced or performed outside New York State, the Omnibus Procurement Act 1994 and 2000 amendments (Chapter 684 and Chapter 383, respectively) require that they be denied contracts which they would otherwise obtain. NOTE: As of May 15, 2002, the list of discriminatory jurisdictions subject to this provision includes the states of South Carolina, Alaska, West Virginia, Wyoming, Louisiana and Hawaii. Contact NYS Department of Economic Development for a current list of jurisdictions subject to this provision.

22. COMPLIANCE WITH NEW YORK STATE INFORMATION SECURITY BREACH AND NOTIFICATION ACT.

Contractor shall comply with the provisions of the New York State Information Security Breach and Notification Act (General Business Law Section 899-aa; State Technology Law Section 208).

23. COMPLIANCE WITH CONSULTANT DISCLOSURE LAW.

If this is a contract for consulting services, defined for purposes of this requirement to include analysis, evaluation, research, training, data processing, computer programming, engineering, environmental, health, and mental health services, accounting, auditing, paralegal, legal or similar services, then, in accordance with Section 163 (4-g) of the State Finance Law (as amended by Chapter 10 of the Laws of 2006), the Contractor shall timely, accurately and properly comply with the requirement to submit an annual employment report for the contract to the agency that awarded the contract, the Department of Civil Service and the State Comptroller.

24. PROCUREMENT LOBBYING. To the extent this agreement is a "procurement contract" as defined by State Finance Law Sections 139-j and 139-k, by signing this agreement the contractor certifies and affirms that all disclosures made in accordance with State Finance Law Sections 139-j and 139-k are complete, true and accurate. In the event such certification is found to be intentionally false or intentionally incomplete, the State may terminate the agreement by providing written notification to the Contractor in accordance with the terms of the agreement.

25. CERTIFICATION OF REGISTRATION TO COLLECT SALES AND COMPENSATING USE TAX BY CERTAIN STATE CONTRACTORS, AFFILIATES AND SUBCONTRACTORS.

To the extent this agreement is a contract as defined by Tax Law Section 5-a, if the contractor fails to make the certification required by Tax Law Section 5-a or if during the term of the contract, the Department of Taxation and Finance or the covered agency, as defined by Tax Law 5-a, discovers that the certification, made under penalty of perjury, is false, then such failure to file or false certification shall be a material breach of this contract and this contract may be terminated, by providing written notification to the Contractor in accordance with the terms of the agreement, if the covered agency determines that such action is in the best interest of the State.

26. IRAN DIVESTMENT ACT. By entering into this Agreement, Contractor certifies in accordance with State Finance Law §165-a that it is not on the "Entities Determined to be Non-Responsive Bidders/Offerers pursuant to the New York State Iran Divestment Act of 2012" ("Prohibited Entities List") posted at: <http://www.ogs.ny.gov/about/regs/docs/ListofEntities.pdf>

Contractor further certifies that it will not utilize on this Contract any subcontractor that is identified on the Prohibited Entities List. Contractor agrees that should it seek to renew or extend this Contract, it must provide the same certification at the time the Contract is renewed or extended. Contractor also agrees that any proposed Assignee of this Contract will be

January 2014

required to certify that it is not on the Prohibited Entities List before the contract assignment will be approved by the State.

During the term of the Contract, should the state agency receive information that a person (as defined in State Finance Law §165-a) is in violation of the above-referenced certifications, the state agency will review such information and offer the person an opportunity to respond. If the person fails to demonstrate that it has ceased its engagement in the investment activity which is in violation of the Act within 90 days after the determination of such violation, then the state agency shall take such action as may be appropriate and provided for by law, rule, or contract, including, but not limited to, imposing sanctions, seeking compliance, recovering damages, or declaring the Contractor in default.

The state agency reserves the right to reject any bid, request for assignment, renewal or extension for an entity that appears on the Prohibited Entities List prior to the award, assignment, renewal or extension of a contract, and to pursue a responsibility review with respect to any entity that is awarded a contract and appears on the Prohibited Entities list after contract award.

This Page Intentionally Blank

Appendix B

GENERAL SPECIFICATIONS

PLEASE RETAIN THIS DOCUMENT FOR FUTURE REFERENCE

TABLE OF CONTENTS

<u>GENERAL</u>	<u>PAGE</u>	<u>TERMS & CONDITIONS</u>	<u>PAGE</u>
1. Applicability	1	43. Emergency Contracts	9
2. Governing Law	1	44. Purchase Orders	9
3. Ethics Compliance	1	45. (RESERVED)	10
4. (RESERVED)	1	46. (RESERVED)	10
5. Definitions	1-3	47. (RESERVED)	10
		48. Title and Risk of Loss	10
<u>BID SUBMISSION</u>		49. (RESERVED)	10
6. International Bidding	3	50. (RESERVED)	10
7. Bid Opening	3	51. (RESERVED)	10
8. Bid Submission	3	52. Installation	10
9. (RESERVED)	3	53. Repaired or Replaced Product/ Components	11
10. (RESERVED)	4	54. On-Site Storage	11
11. (RESERVED)	4	55. Employees/Subcontractors/Agents	11
12. Bid Contents	4	56. Assignment	11
13. Extraneous Terms	4	57. Subcontractors and Suppliers	11
14. Confidential/Trade Secret Materials	4	58. Performance/Bid Bond	11
15. Release of Bid Evaluation Materials	4	59. Suspension of Work	11
16. Freedom of Information Law	5	60. Termination	11
17. Prevailing Wage Rates - Public Works and Building Services Contracts	5	61. Savings/Force Majeure	12
18. Taxes	6	62. (RESERVED)	12
19. Expenses Prior to Contract Execution	6	63. Default - Authorized User	12
20. Advertising Results	6	64. (RESERVED)	12
21. (RESERVED)	6	65. Remedies for Breach	13
22. Remanufactured, Recycled, Recyclable Or Recovered Materials	6	66. Assignment of Claim	13
23. (RESERVED)	6	67. Toxic Substances	13
24. Pricing	6	68. Independent Contractor	13
25. Drawings	7	69. Security	13
26. Site Inspection	7	70. Cooperation with Third Parties	13
27. Procurement Card	7	71. Contract Term - Renewal	13
28. (RESERVED)	7	72. Additional Warranties	13
		73. Legal Compliance	15
		74. Indemnification	15
		75. Indemnification Relating to Third Party Rights	15
		76. Limitation of Liability	15
		77. Insurance	15
<u>BID EVALUATION</u>		<u>THE FOLLOWING CLAUSES PERTAIN TO TECHNOLOGY & NEGOTIATED CONTRACTS</u>	
29. Bid Evaluation	8	78. Software License Grant	15
30. (RESERVED)	8	79. Product Acceptance	17
31. Clarification/Revisions	8	80. Audit of Licensed Product Usage	17
32. Prompt Payment Discounts	8	81. Ownership/Title to Project Deliverables	17
33. Equivalent or Identical Bids	8	82. Proof of License	18
34. Performance and Responsibility Qualifications	8	83. Product Version	18
35. Disqualification for Past Performance	8	84. Changes to Product or Service Offerings	18
36. Quantity Changes Prior To Award	8	85. No Hardstop/Passive License Monitoring	19
37. Timeframe for Offers	8	86. Source Code Escrow for Licensed Product	19
<u>TERMS & CONDITIONS</u>			
38. Contract Creation/Execution	8		
39. Participation in Centralized Contracts	8		
40. Modification of Contract Terms	9		
41. Scope Changes	9		
42. (RESERVED)	9		

GENERAL

1. APPLICABILITY The terms and conditions set forth in this Appendix B are expressly incorporated in and applicable to the resulting procurement contracts let by the Office of General Services Procurement Services Group, or let by any other Authorized User where incorporated by reference in its Bid Documents. Captions are intended as descriptive and are not intended to limit or otherwise restrict the terms and conditions set forth herein.

2. GOVERNING LAW This procurement, the resulting contract and any purchase orders issued hereunder shall be governed by the laws of the State of New York except where the Federal supremacy clause requires otherwise, and actions or proceedings arising from the contract shall be heard in a court of competent jurisdiction in the State of New York.

3. ETHICS COMPLIANCE All Bidders/Contractors and their employees must comply with the requirements of Sections 73 and 74 of the Public Officers Law, other State codes, rules, regulations and executive orders establishing ethical standards for the conduct of business with New York State. In signing the Bid, Bidder certifies full compliance with those provisions for any present or future dealings, transactions, sales, contracts, services, offers, relationships, etc., involving New York State and/or its employees. Failure to comply with those provisions may result in disqualification from the Bidding process, termination of contract, and/or other civil or criminal proceedings as required by law.

4. (RESERVED)

5. DEFINITIONS Terms used in this Appendix B shall have the following meanings:

AFFILIATE Any individual or other legal entity, (including but not limited to sole proprietor, partnership, limited liability company, firm or corporation) that effectively controls another company in which (a) the Bidder owns more than 50% of the ownership; or (b) any individual or other legal entity which owns more than 50% of the ownership of the Bidder. In addition, if a Bidder owns less than 50% of the ownership of another legal entity, but directs or has the right to direct such entity's daily operations, that entity will be an Affiliate.

AGENCY OR AGENCIES The State of New York, acting by or through one or more departments, boards, commissions, offices or institutions of the State of New York.

ATTORNEY GENERAL Attorney General of the State of New York.

BID OR BID PROPOSAL An offer or proposal submitted by a Bidder to furnish a described product or a solution, perform services or means of achieving a practical end, at a stated price for the stated Contract term. As required by the Bid Documents, the Bid or proposal may be subject to modification through the solicitation by the Agency of best and final offers during the evaluation process prior to recommendation for award of the Contract.

BIDDER/OFFERER Any individual or other legal entity (including but not limited to sole proprietor, partnership, limited liability company, firm or corporation) which submits a Bid in response to a Bid Solicitation. The term Bidder shall also include the term "offeror." In the case of negotiated Contracts, "Bidder" shall refer to the "Contractor."

BID DOCUMENTS Writings by the State setting forth the scope, terms, conditions and technical specifications for a procurement of Product. Such writings typically include, but are not limited to: Invitation for Bids (IFB), Request for Quotation (RFQ), Request for Proposals (RFP), addenda or amendments thereto, and terms and conditions which are incorporated by reference, including but not limited to, Appendix A (Standard Clauses for NYS Contracts), and Appendix B, (General Specifications). Where these General Specifications are incorporated in negotiated Contracts that have not been competitively Bid, the term "Bid Documents" shall be deemed to refer to the terms and conditions set forth in the negotiated Contract and associated documentation.

BID SPECIFICATION A written description drafted by the Authorized User setting forth the specific terms of the intended procurement, which may include: physical or functional characteristics, the nature of a commodity or construction item, any description of the work to be performed, Products to be provided, the necessary qualifications of the Bidder, the capacity and capability of the Bidder to successfully carry out the proposed Contract, or the process for achieving specific results and/or anticipated outcomes or any other requirement necessary to perform work. Where these General Specifications are incorporated in negotiated Contracts that have not been competitively Bid, the term "Bid Specifications" shall be deemed to refer to the terms and conditions set forth in the negotiated Contract and associated documentation.

COMMISSIONER Commissioner of OGS, or in the case of Bid Specifications issued by an Authorized User, the head of such Authorized User or their authorized representative.

COMPTROLLER Comptroller of the State of New York.

CONTRACT The writing(s) which contain the agreement of the Commissioner and the Bidder/Contractor setting forth the total legal obligation between the parties as determined by applicable rules of law, and which most typically include the following classifications of public procurements:

a. Agency Specific Contracts Contracts where the specifications for a Product or a particular scope of work are described and defined to meet the needs of one or more Authorized User(s).

b. Centralized Contracts Single or multiple award Contracts where the specifications for a Product or general scope of work are described and defined by the Office of General Services to meet the needs of Authorized Users. Centralized Contracts may be awarded through multiple awards or through adoption of another jurisdiction's contract or on a sole source, single source, emergency or competitive basis. Once established, procurements may be made from the selected Contractor(s) without further competition or Mini-Bid unless otherwise required by the Bid Specifications or Contract Award Notification.

c. Back-Drop Contracts Multiple award Centralized Contracts where the Office of General Services defines the specifications for a Product or general scope of work to meet the needs of Authorized Users. Bids may be submitted either at a date and time certain or may be accepted on a continuous or periodic recruitment basis, as set forth in the Bid Specifications. Selection of a Contractor(s) from among Back-Drop contract holders for an actual Product, project or particular scope of work may subsequently be made on a single or sole source basis, or on the basis of a Mini-Bid among qualified Back-Drop contract holders, or such other method as set forth in the Bid Document.

d. Piggyback Contract A Contract let by any department, agency or instrumentality of the United States government, or any department, agency, office, political subdivision or instrumentality of any state or state(s) which is adopted and extended for use by the OGS Commissioner in accordance with the requirements of the State Finance Law.

e. Contract Letter A letter to the successful Bidder(s) indicating acceptance of its Bid in response to a solicitation. Unless otherwise specified, the issuance of a Letter of Acceptance forms a Contract but is not an order for Product, and Contractor should not take any action with respect to actual Contract deliveries except on the basis of Purchase Orders sent from Authorized User(s).

CONTRACT AWARD NOTIFICATION An announcement to Authorized Users that a Contract has been established.

CONTRACTOR Any successful Bidder(s) to whom a Contract has been awarded by the Commissioner.

DOCUMENTATION The complete set of manuals (e.g., user, installation, instruction or diagnostic manuals) in either hard or electronic copy, which are necessary to enable an Authorized User to properly test, install, operate and enjoy full use of the Product.

EMERGENCY An urgent and unexpected requirement where health and public safety or the conservation of public resources is at risk.

ENTERPRISE The total business operations in the United States of Authorized User (s) without regard to geographic location where such operations are performed or the entity actually performing such operations on behalf of Authorized User.

ENTERPRISE LICENSE A license grant of unlimited rights to deploy, access, use and execute Product anywhere within the Enterprise up to the maximum capacity stated on the Purchase Order or in the Contract.

ERROR CORRECTIONS Machine executable software code furnished by Contractor which corrects the Product so as to conform to the applicable warranties, performance standards and/or obligations of the Contractor.

GROUP A classification of Product, services or technology which is designated by OGS.

INVITATION FOR BIDS (IFB) A type of Bid Document which is most typically used where requirements can be stated and award will be made based on lowest price to the responsive and responsible Bidder(s).

LICENSED SOFTWARE Software transferred upon the terms and conditions set forth in the Contract. "Licensed Software" includes error corrections, upgrades, enhancements or new releases, and any deliverables due under a maintenance or service contract (e.g., patches, fixes, PTFs, programs, code or data conversion, or custom programming).

LICENSEE One or more Authorized Users who acquire Product from Contractor by issuing a Purchase Order in accordance with the terms and conditions of the Contract; provided that, for purposes of compliance with an individual license, the term "Licensee" shall be deemed to refer separately to the individual Authorized User(s) who took receipt of and who is executing the Product, and who shall be solely responsible for performance and liabilities incurred. In the case

of acquisitions by State Agencies, the Licensee shall be the State of New York.

LICENSE EFFECTIVE DATE The date Product is delivered to an Authorized User. Where a License involves Licensee's right to copy a previously licensed and delivered Master Copy of a Program, the license effective date for additional copies shall be deemed to be the date on which the Purchase Order is executed.

LICENSOR A Contractor who transfers rights in proprietary Product to Authorized Users in accordance with the rights and obligations specified in the Contract.

MINI-BID PROJECT DEFINITION A Bid Document containing project specific Bid Specifications developed by or for an Authorized User which solicits Bids from Contractors previously qualified under a Back-Drop Contract.

MULTIPLE AWARD A determination and award of a Contract in the discretion of the Commissioner to more than one responsive and responsible Bidder who meets the requirements of a specification, where the multiple award is made on the grounds set forth in the Bid Document in order to satisfy multiple factors and needs of Authorized Users (e.g., complexity of items, various manufacturers, differences in performance required to accomplish or produce required end results, production and distribution facilities, price, compliance with delivery requirements, geographic location or other pertinent factors).

NEW PRODUCT RELEASES (Product Revisions) Any commercially released revisions to the licensed version of a Product as may be generally offered and available to Authorized Users. New releases involve a substantial revision of functionality from a previously released version of the Product.

OGS The New York State Office of General Services.

PROCUREMENT RECORD Documentation by the Authorized User of the decisions made and approach taken during the procurement process and during the contract term.

PRODUCT A deliverable under any Bid or Contract which may include commodities, services and/or technology. The term "Product" includes Licensed Software.

PROPRIETARY Protected by secrecy, patent, copyright or trademark against commercial competition.

PURCHASE ORDER The Authorized User's fiscal form or format that is used when making a purchase (e.g., formal written Purchase Order, Procurement Card, electronic Purchase Order, or other authorized instrument).

REQUEST FOR PROPOSALS (RFP) A type of Bid Document that is used for procurements where factors in addition to cost are considered and weighted in awarding the contract and where the method of award is "best value," as defined by the State Finance Law.

REQUEST FOR QUOTATION (RFQ) A type of Bid Document that can be used when a formal Bid opening is not required (e.g., discretionary, sole source, single source or emergency purchases).

RESPONSIBLE BIDDER A Bidder that is determined to have financial and organizational capacity, legal authority, satisfactory previous performance, skill, judgment and integrity, and that is found to be competent, reliable and experienced, as determined by the Commissioner. For purposes of being deemed responsible, a Bidder

must also be determined to be in compliance with Sections 139-j and 139-k of the State Finance Law relative to restrictions on contacts during the procurement process and disclosure of contacts and prior findings of non-responsibility under these statutes.

RESPONSIVE BIDDER A Bidder meeting the specifications or requirements prescribed in the Bid Document or solicitation, as determined by the OGS Commissioner.

SINGLE SOURCE A procurement where two or more Bidders can supply the required Product, and the Commissioner may award the contract to one Bidder over the other.

SITE The location (street address) where Product will be executed or services delivered.

SOLE SOURCE A procurement where only one Bidder is capable of supplying the required Product.

SOURCE CODE The programming statements or instructions written and expressed in any language understandable by a human being skilled in the art which are translated by a language compiler to produce executable machine Object Code.

STATE State of New York.

SUBCONTRACTOR Any individual or other legal entity, (including but not limited to sole proprietor, partnership, limited liability company, firm or corporation) who has entered into a contract, express or implied, for the performance of a portion of a Contract with a Contractor.

TERMS OF LICENSE The terms and conditions set forth in the Contract that are in effect and applicable to a Purchase Order at the time of order placement.

VIRUS Any computer code, whether or not written or conceived by Contractor, that disrupts, disables, harms, or otherwise impedes in any manner the operation of the Product, or any other associated software, firmware, hardware, or computer system (such as local area or wide-area networks), including aesthetic disruptions or distortions, but does not include security keys or other such devices installed by Product manufacturer.

BID SUBMISSION

6. INTERNATIONAL BIDDING All offers (tenders), and all information and Product required by the solicitation or provided as explanation thereof, shall be submitted in English. All prices shall be expressed, and all payments shall be made, in United States Dollars (\$US). Any offers (tenders) submitted which do not meet the above criteria will be rejected.

7. BID OPENING Bids may, as applicable, be opened publicly. The Commissioner reserves the right at any time to postpone or cancel a scheduled Bid opening.

8. BID SUBMISSION All Bids are to be packaged, sealed and submitted to the location stated in the Bid Specifications. Bidders are solely responsible for timely delivery of their Bids to the location set forth in the Bid Specifications prior to the stated Bid opening date/time.

A Bid return envelope, if provided with the Bid Specifications, should be used with the Bid sealed inside. If the Bid response does not fit into

the envelope, the Bid envelope should be attached to the outside of the sealed box or package with the Bid inside. If using a commercial delivery company that requires use of their shipping package or envelope, Bidder's sealed Bid, labeled as detailed below, should be placed within the shipper's sealed envelope to ensure that the Bid is not prematurely opened.

All Bids must have a label on the outside of the package or shipping container outlining the following information:

"BID ENCLOSED (bold print, all capitals)

- Group Number
- IFB or RFP Number
- Bid Submission date and time"

In the event that a Bidder fails to provide such information on the return Bid envelope or shipping material, the receiving entity reserves the right to open the shipping package or envelope to determine the proper Bid number or Product group, and the date and time of Bid opening. Bidder shall have no claim against the receiving entity arising from such opening and such opening shall not affect the validity of the Bid or the procurement.

Notwithstanding the receiving agency's right to open a Bid to ascertain the foregoing information, Bidder assumes all risk of late delivery associated with the Bid not being identified, packaged or labeled in accordance with the foregoing requirements.

All Bids must be signed by a person authorized to commit the Bidder to the terms of the Bid Documents and the content of the Bid (offer).

9. (RESERVED)

10. (RESERVED)

11. (RESERVED)

12. BID CONTENTS Bids must be complete and legible. All Bids must be signed. All information required by the Bid Specifications must be supplied by the Bidder on the forms or in the format specified. No alteration, erasure or addition is to be made to the Bid Documents. Changes may be ignored by the Commissioner or may be grounds for rejection of the Bid. Changes, corrections and/or use of white-out in the Bid or Bidder's response portion of the Bid Document must be initialed by an authorized representative of the Bidder. Bidders are cautioned to verify their Bids before submission, as amendments to Bids or requests for withdrawal of Bids received by the Commissioner after the time specified for the Bid opening, may not be considered.

13. EXTRANEIOUS TERMS Bids must conform to the terms set forth in the Bid Documents, as extraneous terms or material deviations (including additional, inconsistent, conflicting or alternative terms) may render the Bid non-responsive and may result in rejection of the Bid.

Extraneous term(s) submitted on standard, pre-printed forms (including but not limited to: product literature, order forms, license agreements, contracts or other documents) that are attached or referenced with submissions shall not be considered part of the Bid or resulting Contract, but shall be deemed included for informational or promotional purposes only.

Only those extraneous terms that meet all the following requirements may be considered as having been submitted as part of the Bid:

a. Each proposed extraneous term (addition, deletion, counter-offer, deviation, or modification) must be specifically enumerated in a writing which is not part of a pre-printed form; and

b. The writing must identify the particular specification requirement (if any) that Bidder rejects or proposes to modify by inclusion of the extraneous term; and

c. The Bidder shall enumerate the proposed addition, counter offer, modification or deviation from the Bid Document, and the reasons therefore.

No extraneous term(s), whether or not deemed "material," shall be incorporated into a Contract or Purchase Order unless submitted in accordance with the above and the Commissioner or Authorized User expressly accepts each such term(s) in writing. Acceptance and/or processing of the Bid shall not constitute such written acceptance of Extraneous Term(s).

14. CONFIDENTIAL/TRADE SECRET MATERIALS

a. **Contractor** Confidential, trade secret or proprietary materials as defined by the laws of the State of New York must be clearly marked and identified as such upon submission by the Bidder. Marking the Bid as "confidential" or "proprietary" on its face or in the document header or footer shall not be considered by the Commissioner or Authorized User to be sufficient without specific justification as to why disclosure of particular information in the Bid would cause substantial injury to the competitive position of the Bidder. Bidders/Contractors intending to seek an exemption from disclosure of these materials under the Freedom of Information Law must request the exemption in writing, setting forth the reasons for the claimed exemption. Acceptance of the claimed materials does not constitute a determination on the exemption request, which determination will be made in accordance with statutory procedures. Properly identified information that has been designated confidential, trade secret, or proprietary by the Bidder will not be disclosed except as may be required by the Freedom of Information Law or other applicable State and federal laws.

b. **Commissioner or Authorized User** Contractor further warrants, covenants and represents that any confidential information obtained by Contractor, its agents, Subcontractors, officers, distributors, resellers or employees in the course of performing its obligations, including without limitation, security procedures, business operations information, or commercial proprietary information in the possession of the State or any Authorized User hereunder or received from another third party, will not be divulged to any third parties. Contractor shall not be required to keep confidential any such material that is publicly available through no fault of Contractor, independently developed by Contractor without reliance on confidential information of the Authorized User, or otherwise obtained under the Freedom of Information Act or other applicable New York State laws and regulations. This warranty shall survive termination of this Contract. Contractor further agrees to take appropriate steps as to its agents, Subcontractors, officers, distributors, resellers or employees regarding the obligations arising under this clause to insure such confidentiality.

15. RELEASE OF BID EVALUATION MATERIALS Requests concerning the evaluation of Bids may be submitted under the Freedom of Information Law. Information, other than statistical or factual tabulations or data such as the Bid Tabulation, shall only be released as required by law after Contract award. Bid Tabulations are not maintained for all procurements. Names of Bidders may be disclosed after Bid opening upon request. Written requests should be directed to the Commissioner.

16. FREEDOM OF INFORMATION LAW During the evaluation process, the content of each Bid will be held in confidence and details of any Bid will not be revealed (except as may be required under the Freedom of Information Law or other State law). The Freedom of Information Law provides for an exemption from disclosure for trade secrets or information the disclosure of which would cause injury to the competitive position of commercial enterprises. This exception would be effective both during and after the evaluation process. If the Bid contains any such trade secret or other confidential or proprietary information, it must be accompanied in the Bid with a written request to the Commissioner to not disclose such information. Such request must state with particularity the reasons why the information should not be available for disclosure and must be provided at the time of submission of the Bid. Notations in the header, footer or watermark of the Bid Document will not be considered sufficient to constitute a request for non-disclosure of trade secret or other confidential or proprietary information. Where a Freedom of Information request is made for trademark or other confidential or proprietary information, the Commissioner reserves the right to determine upon written notice to the Bidder whether such information qualifies for the exemption for disclosure under the law. Notwithstanding the above, where a Bid tabulation is prepared and Bids publicly opened, such Bid tabulation shall be available upon request.

17. PREVAILING WAGE RATES - PUBLIC WORKS AND BUILDING SERVICES CONTRACTS If any portion of work being Bid is subject to the prevailing wage rate provisions of the Labor Law, the following shall apply:

a. "Public Works" and "Building Services" - Definitions

i. **Public Works** Labor Law Article 8 applies to contracts for public improvement in which laborers, workers or mechanics are employed on a "public works" project (distinguished from public "procurement" or "service" contracts). The State, a public benefit corporation, a municipal corporation (including a school district), or a commission appointed by law must be a party to the Contract. The wage and hours provision applies to any work performed by Contractor or Subcontractors.

ii. **Building Services** Labor Law Article 9 applies to Contracts for building service work over \$1,500 with a public agency, that: (i) involve the care or maintenance of an existing building, or (ii) involve the transportation of office furniture or equipment to or from such building, or (iii) involve the transportation and delivery of fossil fuel to such building, and (iv) the principal purpose of which is to furnish services through use of building service employees.

b. **Prevailing Wage Rate Applicable to Bid Submissions** A copy of the applicable prevailing wage rates to be paid or provided are annexed to the Bid Documents. Bidders must submit Bids which are based upon the prevailing hourly wages, and supplements in cash or equivalent benefits (i.e., fringe benefits and any cash or non-cash compensation which are not wages, as defined by law) that equal or exceed the applicable prevailing wage rate(s) for the location where the work is to be performed. Bidders may not submit Bids based upon hourly wage rates and supplements below the applicable prevailing wage rates as established by the New York State Department of Labor. **Bids that fail to comply with this requirement will be disqualified.**

c. **Wage Rate Payments / Changes During Contract Term** The wages to be paid under any resulting Contract shall not be less than the prevailing rate of wages and supplements as set forth by law. It is required that the Contractor keep informed of all changes in the Prevailing Wage Rates during the Contract term that apply to the classes of individuals supplied by the Contractor on any projects resulting from this Contract, subject to the provisions of the Labor

Law. Contractor is solely liable for and must pay such required prevailing wage adjustments during the Contract term as required by law.

d. Public Posting & Certified Payroll Records In compliance with Article 8, Section 220 of the New York State Labor Law:

i. Posting The Contractor must publicly post on the work site, in a prominent and accessible place, a legible schedule of the prevailing wage rates and supplements.

ii. Payroll Records Contractors and Subcontractors must keep original payrolls or transcripts subscribed and affirmed as true under the penalties of perjury as required by law. For public works contracts over \$25,000 where the Contractor maintains no regular place of business in New York State, such records must be kept at the work site. For building services contracts, such records must be kept at the work site while work is being performed.

iii. Submission of Certified Payroll Transcripts for Public Works Contracts Only Contractors and Subcontractors on public works projects must submit monthly payroll transcripts to the Authorized User that has prepared or directs the preparation of the plans and specifications for a public works project, as set forth in the Bid Specifications. For Mini-Bid solicitations, the payroll records must be submitted to the entity preparing the agency Mini-Bid project specification. For "agency specific" Bids, the payroll records should be submitted to the entity issuing the purchase order. For all other OGS Centralized Contracts, such records should be submitted to the individual agency issuing the purchase order(s) for the work. Upon mutual agreement of the Contractor and the Authorized User, the form of submission may be submitted in a specified disk format acceptable to the Department of Labor provided: 1) the Contractor/Subcontractor retains the original records; and, (2) an original signed letter by a duly authorized individual of the Contractor or Subcontractor attesting to the truth and accuracy of the records accompanies the disk. This provision does not apply to Article 9 of the Labor Law building services contracts.

iv. Records Retention Contractors and Subcontractors must preserve such certified transcripts for a period of three years from the date of completion of work on the awarded contract.

Day's Labor Eight hours shall constitute a legal day's work for all classes of employees in this state except those engaged in farm and domestic service unless otherwise provided by law.

No laborers, workmen or mechanics in the employ of the Contractor, Subcontractor or other person doing or contracting to do all or part of the work contemplated by the Contract shall be permitted or required to work more than eight hours in any one calendar day or more than five calendar days in any one week except in cases of extraordinary emergency including fire, flood or danger to life or property. "Extraordinary emergency" shall be deemed to include situations in which sufficient laborers, workers and mechanics cannot be employed to carry on public work expeditiously as a result of such restrictions upon the number of hours and days of labor and the immediate commencement or prosecution or completion without undue delay of the public work is necessary in the judgment of the NYS Commissioner of Labor for the preservation of the Contract site or for the protection of the life and limb of the persons using the Contract site.

18. TAXES

a. Unless otherwise specified in the Bid Specifications or Contract, the quoted Bid price includes all taxes applicable to the transaction.

b. Purchases made by the State of New York and certain non-State Authorized Users are exempt from New York State and local sales taxes and, with certain exceptions, federal excise taxes. To satisfy the requirements of the New York State Sales tax exemption, either the Purchase Order issued by a State Agency or the invoice forwarded to authorize payment for such purchases will be sufficient evidence that the sale by the Contractor was made to the State, an exempt organization under Section 1116 (a) (1) of the Tax Law. Non-State Authorized Users must offer their own proof of exemption upon request. No person, firm or corporation is, however, exempt from paying the State Truck Mileage and Unemployment Insurance or Federal Social Security taxes, which remain the sole responsibility of the Bidder/Contractor.

c. Pursuant to Revised Tax Law 5-a, Contractor will be required to furnish sales tax certification on its behalf and for its affiliates, and subcontractors for Contracts with a value greater than \$100,000 in accordance with provisions of the law.

d. Purchases by Authorized Users other than the State of New York may be subject to certain taxes which were not included in the Bid price, and in those instances the tax should be computed based on the Contract price and added to the invoice submitted to such entity for payment.

19. EXPENSES PRIOR TO CONTRACT EXECUTION The Commissioner and any Authorized User(s) are not liable for any costs incurred by a Vendor, Bidder or Contractor in the preparation and production of a Bid, Mini-Bid or best and final offers or for any work performed prior to Contract execution.

20. ADVERTISING RESULTS The prior written approval of the Commissioner is required in order for results of the Bid to be used by the Contractor as part of any commercial advertising. The Contractor shall also obtain the prior written approval of the Commissioner relative to the Bid or Contract for press or other media releases.

21. (RESERVED)

22. REMANUFACTURED, RECYCLED, RECYCLABLE OR RECOVERED MATERIALS Upon the conditions specified in the Bid Specifications and in accordance with the laws of the State of New York, Contractors are encouraged to use recycled, recyclable or recovered materials in the manufacture of Products and packaging to the maximum extent practicable without jeopardizing the performance or intended end use of the Product or packaging unless such use is precluded due to health, welfare, safety requirements or in the Bid Specifications. Contractors are further encouraged to offer remanufactured Products to the maximum extent practicable without jeopardizing the performance or intended end use of the Product and unless such use is precluded due to health, welfare, safety requirements or by the Bid Specifications. Where such use is not practical, suitable, or permitted by the Bid Specifications, Contractor shall deliver new materials in accordance with the "Warranties" set forth below.

Items with recycled, recyclable, recovered, refurbished or remanufactured content must be identified in the Bid or Bidder will be deemed to be offering new Product.

23. (RESERVED)

24. PRICING

a. **Unit Pricing** If required by the Bid Specifications, the Bidder should insert the price per unit specified and the price extensions in

decimals, not to exceed four places for each item unless otherwise specified, in the Bid. In the event of a discrepancy between the unit price and the extension, the unit price shall govern unless, in the sole judgment of the Commissioner, such unit pricing is obviously erroneous.

b. Net Pricing Unless otherwise required by the Bid Specifications, prices shall be net, including transportation, customs, tariff, delivery and other charges fully prepaid by the Contractor to the destination(s) indicated in the Bid Specifications, subject to the cash discount.

c. “No Charge” Bid When Bids are requested on a number of Products as a Group or Lot, a Bidder desiring to Bid “no charge” on a Product in the Group or Lot must clearly indicate such. Otherwise, such Bid may be considered incomplete and be rejected, in whole or in part, at the discretion of the Commissioner.

d. Educational Pricing All Products to be supplied for educational purposes that are subject to educational discounts shall be identified in the Bid and such discounts shall be made available to qualifying institutions.

e. Third Party Financing If Product acquisitions are financed through any third party financing, Contractor may be required as a condition of Contract Award to agree to the terms and conditions of a “Consent & Acknowledgment Agreement” in a form acceptable to the Commissioner.

f. Best Pricing Offer During the Contract term, if substantially the same or a smaller quantity of a Product is sold by the Contractor outside of this Contract upon the same or similar terms and conditions as that of this Contract at a lower price to a federal, state or local governmental entity, the price under this Contract, at the discretion of the Commissioner, shall be immediately reduced to the lower price.

Price decreases shall take effect automatically during the Contract term and apply to Purchase Orders submitted on or after:

(i) GSA Changes: Where NYS Net Prices are based on an approved GSA Schedule, the date the approved GSA Schedule pricing decreases during the Contract term; or

(ii) Commercial Price List Reductions: Where NYS Net Prices are based on a discount from Contractor’s list prices, the date Contractor lowers its pricing to its customers generally or to similarly situated government customers during the Contract term; or

(iii) Special Offers/Promotions Generally: Where Contractor generally offers more advantageous special price promotions or special discount pricing to other customers during the Contract term for a similar quantity, and the maximum price or discount associated with such offer or promotion is better than the discount or Net Price otherwise available under this Contract, such better price or discount shall apply for similar quantity transactions under this Contract for the life of such general offer or promotion; and

(iv) Special Offers/Promotions to Authorized Users: Contractor may offer Authorized Users, under either this Contract or any other Contracting vehicle, competitive pricing which is lower than the NYS Net Price set forth herein at any time during the Contract term and such lower pricing shall not be applied as a global price reduction under the Contract pursuant to the foregoing paragraph (iii).

Unless otherwise specified in the Bid Specifications, Contractor may offer lower prices or better terms (see Modification of Contract Terms) on any specific Purchase Order(s) from any Authorized User without being in conflict with, or obligation to comply on a global basis, with the terms of this clause.

g. Best and Final Prices As specified in the Bid Documents and Contract, a Contractor may be solicited at the time of issuance of a Purchase Order or Mini-Bid award for best and final pricing for the Product or service to be delivered to the Authorized User. Contractors are encouraged to reduce their pricing upon receipt of such request.

25. DRAWINGS

a. Drawings Submitted With Bid When the Bid Specifications require the Bidder to furnish drawings and/or plans, such drawings and/or plans shall conform to the mandates of the Bid Documents and shall, when approved by the Commissioner, be considered a part of the Bid and of any resulting Contract. All symbols and other representations appearing on the drawings shall be considered a part of the drawing.

b. Drawings Submitted During the Contract Term Where required to develop, maintain and deliver diagrams or other technical schematics regarding the scope of work, Contractor shall do so on an ongoing basis at no additional charge, and must, as a condition of payment, update drawings and plans during the Contract term to reflect additions, alterations, and deletions. Such drawings and diagrams shall be delivered to the Authorized User’s representative.

c. Accuracy of Drawings Submitted All drawings shall be neat and professional in manner and shall be clearly labeled as to locations and type of product, connections and components. Drawings and diagrams are to be in compliance with accepted drafting standards. Acceptance or approval of such plans shall not relieve the Contractor from responsibility for design or other errors of any sort in the drawings or plans, or from its responsibility for performing as required, furnishing product, services or installation, or carrying out any other requirements of the intended scope of work.

26. SITE INSPECTION Where a site inspection is required by the Bid Specifications or Project Definition, Bidder shall be required to inspect the site, including environmental or other conditions for pre-existing deficiencies that may affect the installed Product, equipment, or environment or services to be provided and, which may affect Bidder’s ability to properly deliver, install or otherwise provide the required Product. All inquiries regarding such conditions shall be made in writing. Bidder shall be deemed to have knowledge of any deficiencies or conditions which such inspection or inquiry might have disclosed. Bidder must provide a detailed explanation with its Bid if additional work is required under this clause in order to properly complete the delivery and installation of the required Product or provide the requested service.

27. PROCUREMENT CARD The State has entered into an agreement for purchasing card services. The Purchasing Card enables Authorized Users to make authorized purchases directly from a Contractor without processing a Purchase Order or Purchase Authorizations. Purchasing Cards are issued to selected employees authorized to purchase for the Authorized User and having direct contact with Contractors. Cardholders can make purchases directly from any Contractor that accepts the Purchasing Card.

The Contractor shall not process a transaction for payment through the credit card clearinghouse until the purchased products have been shipped or services performed. Unless the cardholder requests correction or replacement of a defective or faulty Product in accordance with other Contract requirements, the Contractor shall immediately credit a cardholder’s account for products returned as defective or faulty.

28. (RESERVED)

BID EVALUATION

29. BID EVALUATION The Commissioner reserves the right to accept or reject any and all Bids, or separable portions of offers, and waive technicalities, irregularities, and omissions if the Commissioner determines the best interests of the State will be served. The Commissioner, in his/her sole discretion, may accept or reject illegible, incomplete or vague Bids and his/her decision shall be final. A conditional or revocable Bid which clearly communicates the terms or limitations of acceptance may be considered, and Contract award may be made in compliance with the Bidder's conditional or revocable terms in the offer.

30. (RESERVED)

31. CLARIFICATIONS / REVISIONS Prior to award, the Commissioner reserves the right to seek clarifications, request Bid revisions, or to request any information deemed necessary for proper evaluation of Bids from all Bidders deemed to be eligible for Contract award. Failure to provide requested information may result in rejection of the Bid.

32. PROMPT PAYMENT DISCOUNTS While prompt payment discounts will not be considered in determining the low Bid, the Commissioner may consider any prompt payment discount in resolving Bids which are otherwise tied. However, any notation indicating that the price is net, (e.g., net 30 days), shall be understood to mean only that no prompt payment discount is offered by the Bidder. The imposition of service, interest, or other charges, except pursuant to the provisions of Article 11-A of the State Finance Law, which are applicable in any case, may render the Bid non-responsive and may be cause for its rejection.

33. EQUIVALENT OR IDENTICAL BIDS In the event two offers are found to be substantially equivalent, price shall be the basis for determining the award recipient. If two or more Bidders submit substantially equivalent Bids as to pricing or other factors, the decision of the Commissioner to award a Contract to one or more of such Bidders shall be final.

34. PERFORMANCE AND RESPONSIBILITY QUALIFICATIONS The Commissioner reserves the right to investigate or inspect at any time whether or not the Product, services, qualifications or facilities offered by the Bidder/Contractor meet the requirements set forth in the Bid Specifications/Contract or as set forth during Contract negotiations. Contractor shall at all times during the Contract term remain responsible and responsive. A Bidder/Contractor must be prepared, if requested by the Commissioner, to present evidence of legal authority to do business in New York State, integrity, experience, ability, prior performance, organizational and financial capacity as well as where applicable, a statement as to supply, plant, machinery and capacity of the manufacturer or source for the production, distribution and servicing of the Product offered/Bid. If the Commissioner determines that the conditions and terms of the Bid Documents, Bid Specifications or Contract are not complied with, or that items, services or Product proposed to be furnished do not meet the specified requirements, or that the legal authority, integrity experience, ability, prior performance, organization and financial capacity or facilities are not satisfactory, the Commissioner may reject such Bid or terminate the Contract.

35. DISQUALIFICATION FOR PAST PERFORMANCE AND FINDINGS OF NON-RESPONSIBILITY Bidder may be disqualified from receiving awards if Bidder, or anyone in Bidder's

employment, has previously failed to perform satisfactorily in connection with public Bidding or contracts or is deemed non-responsive.

36. QUANTITY CHANGES PRIOR TO AWARD The Commissioner reserves the right, at any time prior to the award of a specific quantity Contract, to alter in good faith the quantities listed in the Bid Specifications. In the event such right is exercised, the lowest responsible Bidder meeting Bid Specifications will be advised of the revised quantities and afforded an opportunity to extend or reduce its Bid price in relation to the changed quantities. Refusal by the low Bidder to so extend or reduce its Bid price may result in the rejection of its Bid and the award of such Contract to the lowest responsible Bidder who accepts the revised qualifications.

37. TIMEFRAME FOR OFFERS The Commissioner reserves the right to make awards within sixty (60) days after the date of the Bid opening or such other period of time as set forth in the Bid Documents, during which period, Bids must remain firm and cannot be withdrawn. Pursuant to Section 163(9)(e) of the State Finance Law and Section 2-205 of the Uniform Commercial Code when applicable, where an award is not made within the sixty (60) day period or other time specified as set forth in the Bid Documents, the Bids shall remain firm until such later time as either a Contract is awarded or the Bidder delivers to the Commissioner written notice of the withdrawal of its Bid. Any Bid which expressly states therein that acceptance must be made within a shorter specified time, may at the sole discretion of the Commissioner, be accepted or rejected.

TERMS & CONDITIONS

38. CONTRACT CREATION / EXECUTION Except for contracts governed by Article 11-B of the State Finance Law, subject to and upon receipt of all required approvals as set forth in the Bid Specifications a Contract shall be deemed executed and created with the successful Bidder(s), upon the Commissioner's mailing or electronic communication to the address on the Bid/Contract of: (i) the final Contract Award Notice; (ii) a fully executed Contract; or (iii) a Purchase Order authorized by the Commissioner.

39. PARTICIPATION IN CENTRALIZED CONTRACTS The following shall not limit or inhibit the OGS Commissioner's authority under State Finance Law, Section 163 (10) (e) (Piggybacking):

a. Agencies All State Agencies may utilize and purchase under any state Centralized Contract let by the Commissioner, unless the Bid Documents limit purchases to specific State Agencies.

b. Non-State Agency Authorized Users Authorized Users other than State Agencies are permitted to make purchases through state Centralized Contracts where permitted by law, the Contract or the Commissioner.

c. Voluntary Extension Purchase Orders issued against a State Centralized Contract by any Authorized User not provided for in the Bid Specifications shall be honored by the Contractor at its discretion and only with the approval of the OGS Commissioner and any other approvals required by law. Contractors are encouraged to voluntarily extend service Contracts to those additional entities authorized to utilize commodity Contracts under Section 163 (3) (iv) of the State Finance Law.

d. Responsibility for Performance Participation in state Centralized Contracts by Authorized Users is permitted upon the following conditions: (i) the responsibility with regard to performance

of any contractual obligation, covenant, condition or term thereunder by any Authorized User other than State Agencies shall be borne and is expressly assumed by such Authorized User and not by the State; (ii) a breach of the Contract by any particular Authorized User shall neither constitute nor be deemed a breach of the Contract as a whole which shall remain in full force and effect, and shall not affect the validity of the Contract nor the obligations of the Contractor thereunder respecting non-breaching Authorized Users, whether State or otherwise; (iii) for a breach by an Authorized User other than a State Agency, the State specifically and expressly disclaims any and all liability for such breach; and (iv) each non-state agency Authorized User and Contractor guarantees to save the State, its officers, agents and employees harmless from any liability that may be or is imposed by their failure to perform in accordance with its obligations under the Contract.

e. Contract Migration Authorized Users holding individual Contracts with a Contractor at the time that Contractor is awarded a Centralized Contract for the same Products or services shall be permitted to migrate to that Centralized Contract effective with its commencement date. Such migration shall not operate to diminish, alter or eliminate any right that the Authorized User otherwise had under the terms and conditions of their individual Contract.

40. MODIFICATION OF CONTRACT TERMS The terms and conditions set forth in the Contract shall govern all transactions by Authorized User(s) under this Contract. The Contract may only be modified or amended upon mutual written agreement of the Commissioner and Contractor.

The Contractor may, however, offer Authorized User(s) more advantageous pricing, payment, or other terms and conditions than those set forth in the Contract. In such event, a copy of such terms shall be furnished to the Authorized User(s) and Commissioner by the Contractor at the time of such offer.

Other than where such terms are more advantageous for the Authorized User(s) than those set forth in the Contract, no alteration or modification of the terms of the Contract, including substitution of Product, shall be valid or binding against Authorized User(s) unless authorized by the Commissioner or specified in the Contract Award Notification. No such alteration or modification shall be made by unilaterally affixing such terms to Product upon delivery (including, but not limited to, attachment or inclusion of standard pre-printed order forms, product literature, "shrink wrap" terms accompanying software upon delivery, or other documents) or by incorporating such terms onto order forms, purchase orders or other documents forwarded by the Contractor for payment, notwithstanding Authorized User's subsequent acceptance of Product, or that Authorized User has subsequently processed such document for approval or payment.

41. SCOPE CHANGES The Commissioner reserves the right, unilaterally, to require, by written order, changes by altering, adding to or deducting from the Bid Specifications, such changes to be within the general scope of the Contract. The Commissioner may make an equitable adjustment in the Contract price or delivery date if the change affects the cost or time of performance. Such equitable adjustments require the consent of the Contractor, which consent shall not be unreasonably withheld.

42. (RESERVED)

43. EMERGENCY CONTRACTS In the event that a disaster emergency is declared by Executive Order under Section 28 of Article 2-B of the Executive Law, or the Commissioner determines pursuant to his/her authority under Section 163 (10) (b) of the State Finance

Law that an emergency exists requiring the prompt and immediate delivery of Product, the Commissioner reserves the right to obtain such Product from any source, including but not limited to this Contract(s), as the Commissioner in his/her sole discretion determines will meet the needs of such emergency. Contractor shall not be entitled to any claim or lost profits for Product procured from other sources pursuant to this paragraph. The reasons underlying the finding that an emergency exists shall be included in the procurement record.

44. PURCHASE ORDERS Unless otherwise authorized in writing by the Commissioner, no Product is to be delivered or furnished by Contractor until transmittal of an official Purchase Order from the Authorized User. Unless terminated or cancelled pursuant to the authority vested in the Commissioner, Purchase Orders shall be effective and binding upon the Contractor when placed in the mail or electronically transmitted prior to the termination of the contract period, addressed to the Contractor at the address for receipt of orders set forth in the Contract or in the Contract Award Notification.

All Purchase Orders issued pursuant to Contracts let by the Commissioner must bear the appropriate Contract number and, if necessary, required State approvals. As deemed necessary, the Authorized User may confirm pricing and other Product information with the Contractor prior to placement of the Purchase Order. The State reserves the right to require any other information from the Contractor which the State deems necessary in order to complete any Purchase Order placed under the Contract. Unless otherwise specified, all Purchase Orders against Centralized Contracts will be placed by Authorized Users directly with the Contractor and any discrepancy between the terms stated on the vendor's order form, confirmation or acknowledgment, and the Contract terms shall be resolved in favor of the terms most favorable to the Authorized User. Should an Authorized User add written terms and conditions to the Purchase Order that conflict with the terms and conditions of the Contract, the Contractor has the option of rejecting the Purchase Order within five business days of its receipt but shall first attempt to negotiate the additional written terms and conditions in good faith with the Authorized User, or fulfill the Purchase Order. Notwithstanding the above, the Authorized User reserves the right to dispute any discrepancies arising from the presentation of additional terms and conditions with the Contractor.

If, with respect to an Agency Specific Contract let by the OGS Commissioner, a Purchase Order is not received by the Contractor within two weeks after the issuance of a Contract Award Notification, it is the responsibility of the Contractor to request in writing that the appropriate Authorized User forward a Purchase Order. If, thereafter, a Purchase Order is not received within a reasonable period of time, the Contractor shall promptly notify in writing the appropriate purchasing officer in OGS. Failure to timely notify such officer may, in the discretion of the OGS Commissioner and without cost to the State, result in the cancellation of such requirement by the OGS Commissioner with a corresponding reduction in the Contract quantity and price.

45. (RESERVED)

46. (RESERVED)

47. (RESERVED)

48. TITLE AND RISK OF LOSS Notwithstanding the form of shipment, title or other property interest, risk of loss shall not pass from the Contractor to the Authorized User until the Products have been received, inspected and accepted by the receiving entity. Acceptance shall occur within a reasonable time or in accordance with such other defined acceptance period as may be specified in the Bid Specifications or Purchase Order. Mere acknowledgment by

Authorized User personnel of the delivery or receipt of goods (e.g., signed bill of lading) shall not be deemed or construed as acceptance of the Products received. Any delivery of Product that is substandard or does not comply with the Bid Specifications or Contract terms and conditions, may be rejected or accepted on an adjusted price basis, as determined by the Commissioner.

49. (RESERVED)

50. (RESERVED)

51. (RESERVED)

52. INSTALLATION Where installation is required, Contractor shall be responsible for placing and installing the Product in the required locations. All materials used in the installation shall be of good quality and shall be free from any and all defects that would mar the appearance of the Product or render it structurally unsound. Installation includes the furnishing of any equipment, rigging and materials required to install or place the Product in the proper location. The Contractor shall protect the site from damage for all its work and shall repair damages or injury of any kind caused by the Contractor, its employees, officers or agents. If any alteration, dismantling or excavation, etc. is required to effect installation, the Contractor shall thereafter promptly restore the structure or site. Work shall be performed to cause the least inconvenience to the Authorized User(s) and with proper consideration for the rights of other Contractors or workers. The Contractor shall promptly perform its work and shall coordinate its activities with those of other Contractors. The Contractor shall clean up and remove all debris and rubbish from its work as required or directed. Upon completion of the work, the building and surrounding area of work shall be left clean and in a neat, unobstructed condition, and everything in satisfactory repair and order.

53. REPAIRED OR REPLACED PARTS / COMPONENTS

Where the Contractor is required to repair, replace or substitute Product or parts or components of the Product under the Contract, the repaired, replaced or substituted Products shall be subject to all terms and conditions for new parts and components set forth in the Contract including Warranties, as set forth in the Additional Warranties Clause herein. Replaced or repaired Product or parts and components of such Product shall be new and shall, if available, be replaced by the original manufacturer's component or part. Remanufactured parts or components meeting new Product standards may be permitted by the Commissioner or Authorized User. Before installation, all proposed substitutes for the original manufacturer's installed parts or components must be approved by the Authorized User. The part or component shall be equal to or of better quality than the original part or component being replaced.

54. ON-SITE STORAGE With the written approval of the Authorized User, materials, equipment or supplies may be stored at the Authorized User's site at the Contractor's sole risk.

55. EMPLOYEES, SUBCONTRACTORS & AGENTS All employees, Subcontractors or agents performing work under the Contract must be trained staff or technicians who meet or exceed the professional, technical and training qualifications set forth in the Bid Specifications or the Bid Documents, whichever is more restrictive, and must comply with all security and administrative requirements of the Authorized User. The Commissioner reserves the right to conduct a security background check or otherwise approve any employee, Subcontractor or agent furnished by Contractor and to refuse access to or require replacement of any personnel for cause based on, including but not limited to, professional, technical or training qualifications, quality of work or change in security status or non-compliance with Authorized User's security or other requirements. Such approval shall not relieve the Contractor of the obligation to perform all work in compliance with the Contract terms. The Commissioner reserves

the right to reject and/or bar from the facility for cause any employee, Subcontractor, or agents of the Contractor.

56. ASSIGNMENT The Contractor shall not assign, transfer, convey, sublet, or otherwise dispose of the contract or its right, title or interest therein, or its power to execute such contract to any other person, company, firm or corporation in performance of the contract without the prior written consent of the Commissioner or Authorized User (as applicable). Failure to obtain consent to assignment from the Authorized User shall revoke and annul such Contract. Notwithstanding the foregoing, the State shall not hinder, prevent or affect assignment of money by a Contractor for the benefit of its creditors. Prior to a consent to assignment of monies becoming effective, the Contractor shall file a written notice of such monies assignment(s) with the Comptroller. Prior to a consent to assignment of a Contract, or portion thereof, becoming effective, the Contractor shall submit the request to assignment to the Commissioner and seek written agreement from the Commissioner which will be filed with the Comptroller. The Commissioner reserves the right to reject any proposed assignee in his/her discretion.

Upon notice to the Contractor, the Contract may be assigned without the consent of the Contractor to another State Agency or subdivision of the State pursuant to a governmental reorganization or assignment of functions under which the functions are transferred to a successor Agency or to another Agency that assumes OGS responsibilities for the Contract.

57. SUBCONTRACTORS AND SUPPLIERS The Commissioner reserves the right to reject any proposed Subcontractor or supplier for bona fide business reasons, which may include, but are not limited to: they are on the Department of Labor's list of companies with which New York State cannot do business; the Commissioner determines that the company is not qualified; the Commissioner determines that the company is not responsible; the company has previously provided unsatisfactory work or services; the company failed to solicit minority and women's business enterprises (M/WBE) Bidders as required by prior Contracts.

58. PERFORMANCE / BID BOND The Commissioner reserves the right to require a Bidder or Contractor to furnish without additional cost, a performance, payment or Bid bond or negotiable irrevocable letter of credit or other form of security for the faithful performance of the Contract. Where required, such bond or other security shall be in the form prescribed by the Commissioner.

59. SUSPENSION OF WORK The Commissioner, in his/her sole discretion, reserves the right to suspend any or all activities under this Contract, at any time, in the best interests of the Authorized User. In the event of such suspension, the Contractor will be given a formal written notice outlining the particulars of such suspension. Examples of the reason for such suspension include, but are not limited to, a budget freeze or reduction on State spending, declaration of emergency, contract compliance issues or other such circumstances. Upon issuance of such notice, the Contractor is not to accept any Purchase Orders, and shall comply with the suspension order. Activity may resume at such time as the Commissioner issues a formal written notice authorizing a resumption of performance under the Contract.

An Authorized User may issue a formal written notice for the suspension of work for which it has engaged the Contractor for reasons specified in the above paragraph. The written notice shall set forth the reason for such suspension and a copy of the written notice shall be provided to the Commissioner.

60. TERMINATION

a. For Cause: For a material breach that remains uncured for more than thirty (30) days or other specified period after written notice to the Contractor, the Contract or Purchase Order may be terminated by the Commissioner or Authorized User at the Contractor's expense where Contractor becomes unable or incapable of performing, or meeting any requirements or qualifications set forth in the Contract, or for non-performance, or upon a determination that Contractor is non-responsible. Such termination shall be upon written notice to the Contractor. In such event, the Commissioner or Authorized User may complete the contractual requirements in any manner it may deem advisable and pursue available legal or equitable remedies for breach.

b. For Convenience: By written notice, this Contract may be terminated at any time by the State for convenience upon sixty (60) days written notice or other specified period without penalty or other early termination charges due. Such termination of the Contract shall not affect any project or Purchase Order that has been issued under the Contract prior to the date of such termination. If the Contract is terminated pursuant to this subdivision, the Authorized User shall remain liable for all accrued but unpaid charges incurred through the date of the termination. Contractor shall use due diligence and provide any outstanding deliverables.

c. For Violation of the Sections 139-j and 139-k of the State Finance Law: The Commissioner reserves the right to terminate the Contract in the event it is found that the certification filed by the Bidder in accordance with Section 139-k of the State Finance Law was intentionally false or intentionally incomplete. Upon such finding, the Commissioner may exercise its termination right by providing written notification to the Contractor in accordance with the written notification terms of the Contract.

d. For Violation of Revised Tax Law 5a: The Commissioner reserves the right to terminate the contract in the event it is found that the certification filed by the Contractor in accordance with §5-a of the Tax Law is not timely filed during the term of the Contract or the certification furnished was intentionally false or intentionally incomplete. Upon such finding, the Commissioner may exercise its termination right by providing written notification to the Contractor.

61. SAVINGS/FORCE MAJEURE A force majeure occurrence is an event or effect that cannot be reasonably anticipated or controlled. Force majeure includes, but is not limited to, acts of God, acts of war, acts of public enemies, strikes, fires, explosions, actions of the elements, floods, or other similar causes beyond the control of the Contractor or the Commissioner in the performance of the Contract which non-performance, by exercise of reasonable diligence, cannot be prevented. Contractor shall provide the Commissioner with written notice of any force majeure occurrence as soon as the delay is known.

Neither the Contractor nor the Commissioner shall be liable to the other for any delay in or failure of performance under the Contract due to a force majeure occurrence. Any such delay in or failure of performance shall not constitute default or give rise to any liability for damages. The existence of such causes of such delay or failure shall extend the period for performance to such extent as determined by the Contractor and the Commissioner to be necessary to enable complete performance by the Contractor if reasonable diligence is exercised after the cause of delay or failure has been removed.

Notwithstanding the above, at the discretion of the Commissioner where the delay or failure will significantly impair the value of the Contract to the State or to Authorized Users, the Commissioner may:

a. Accept allocated performance or deliveries from the Contractor. The Contractor, however, hereby agrees to grant preferential treatment

to Authorized Users with respect to Product subjected to allocation; and/or

b. Purchase from other sources (without recourse to and by the Contractor for the costs and expenses thereof) to replace all or part of the Products which are the subject of the delay, which purchases may be deducted from the Contract quantities without penalty or liability to the State; or

c. Terminate the Contract or the portion thereof which is subject to delays, and thereby discharge any unexecuted portion of the Contract or the relative part thereof.

In addition, the Commissioner reserves the right, in his/her sole discretion, to make an equitable adjustment in the Contract terms and/or pricing should extreme and unforeseen volatility in the marketplace affect pricing or the availability of supply. "Extreme and unforeseen volatility in the marketplace" is defined as market circumstances which meet the following criteria: (i) the volatility is due to causes outside the control of Contractor; (ii) the volatility affects the marketplace or industry, not just the particular Contract source of supply; (iii) the effect on pricing or availability of supply is substantial; and (iv) the volatility so affects Contractor's performance that continued performance of the Contract would result in a substantial loss.

62. (RESERVED)

63. DEFAULT – AUTHORIZED USER

a. Breach of Authorized User Not Breach of Centralized Contract. An Authorized User's breach shall not be deemed a breach of the Centralized Contract, rather it shall be deemed a breach of the Authorized User's performance under the terms and conditions of the Centralized Contract.

b. Failure to Make Payment. In the event a participating Authorized User fails to make payment to the Contractor for Products delivered, accepted and properly invoiced, within 60 days of such delivery and acceptance, the Contractor may, upon 10 days advance written notice to both the Commissioner and the Authorized User's purchasing official, suspend additional shipments of Product or provision of services to such entity until such time as reasonable arrangements have been made and assurances given by such entity for current and future Contract payments.

c. Notice of Breach. Notwithstanding the foregoing, the Contractor shall, at least 10 days prior to declaring a breach of Contract by any Authorized User, by certified or registered mail, notify both the Commissioner and the purchasing official of the breaching Authorized User of the specific facts, circumstances and grounds upon which a breach will be declared.

d. It is understood, however, that if the Contractor's basis for declaring a breach is insufficient, the Contractor's declaration of breach and failure to service an Authorized User shall constitute a breach of its Contract and the Authorized User may thereafter seek any remedy available at law or equity.

64. (RESERVED)

65. REMEDIES FOR BREACH It is understood and agreed that all rights and remedies afforded below shall be in addition to all remedies or actions otherwise authorized or permitted by law:

a. Cover/Substitute Performance In the event of Contractor's material breach, the Commissioner may, with or without formally

Bidding: (i) Purchase from other sources; or (ii) If the Commissioner is unsuccessful after making reasonable attempts, under the circumstances then existing, to timely obtain acceptable service or acquire replacement Product of equal or comparable quality, the Commissioner may acquire acceptable replacement Product of lesser or greater quality.

Such purchases may, in the discretion of the Commissioner, be deducted from the Contract quantity and payments due Contractor.

b. Withhold Payment In any case where a question of non-performance by Contractor arises, payment may be withheld in whole or in part at the discretion of the Commissioner. Should the amount withheld be finally paid, a cash discount originally offered may be taken as if no delay in payment had occurred.

c. Bankruptcy In the event that the Contractor files a petition under the U.S. Bankruptcy Code during the term of this Centralized Contract, Authorized Users may, at their discretion, make application to exercise its right to set-off against monies due the Debtor or, under the Doctrine of Recoupment, credit the Authorized User the amounts owed by the Contractor arising out of the same transactions.

d. Reimbursement of Costs Incurred The Contractor agrees to reimburse the Authorized User promptly for any and all additional costs and expenses incurred for acquiring acceptable services, and/or replacement Product. Should the cost of cover be less than the Contract price, the Contractor shall have no claim to the difference. The Contractor covenants and agrees that in the event suit is successfully prosecuted for any default on the part of the Contractor, all costs and expenses expended or incurred by the Authorized User in connection therewith, including reasonable attorney's fees, shall be paid by the Contractor.

Where the Contractor fails to timely deliver pursuant to the guaranteed delivery terms of the Contract, the ordering Authorized User may rent substitute equipment temporarily. Any sums expended for such rental shall, upon demand, be reimbursed to the Authorized User promptly by the Contractor or deducted by the Authorized User from payments due or to become due the Contractor on the same or another transaction.

e. Deduction/Credit Sums due as a result of these remedies may be deducted or offset by the Authorized User from payments due, or to become due, the Contractor on the same or another transaction. If no deduction or only a partial deduction is made in such fashion the Contractor shall pay to the Authorized User the amount of such claim or portion of the claim still outstanding, on demand. The Commissioner reserves the right to determine the disposition of any rebates, settlements, restitution, liquidated damages, etc., which arise from the administration of the Contract.

66. ASSIGNMENT OF CLAIM Contractor hereby assigns to the State any and all its claims for overcharges associated with this Contract which may arise under the antitrust laws of the United States, 15 USC Section 1, et. seq. and the antitrust laws of the State of New York, General Business Law Section 340, et. seq.

67. TOXIC SUBSTANCES Each Contractor furnishing a toxic substance as defined by Section 875 of the Labor Law, shall provide such Authorized User with not less than two copies of a material safety data sheet, which sheet shall include for each such substance the information outlined in Section 876 of the Labor Law.

Before any chemical product is used or applied on or in any building, a copy of the product label and Material Safety Data Sheet must be provided to and approved by the Authorized User agency representative.

68. INDEPENDENT CONTRACTOR It is understood and agreed that the legal status of the Contractor, its agents, officers and employees under this Contract is that of an independent Contractor, and in no manner shall they be deemed employees of the Authorized User, and therefore are not entitled to any of the benefits associated with such employment. The Contractor agrees, during the term of this Contract, to maintain at Contractor's expense those benefits to which its employees would otherwise be entitled by law, including health benefits, and all necessary insurance for its employees, including worker's compensation, disability and unemployment insurance, and to provide the Authorized User with certification of such insurance upon request. The Contractor remains responsible for all applicable federal, state and local taxes, and all FICA contributions.

69. SECURITY Contractor warrants, covenants and represents that it will comply fully with all security procedures of the Authorized User(s) in performance of the Contract including but not limited to physical, facility, documentary and cyber security rules, procedures and protocols.

70. COOPERATION WITH THIRD PARTIES The Contractor shall be responsible for fully cooperating with any third party, including but not limited to other Contractors or Subcontractors of the Authorized User, as necessary to ensure delivery of Product or coordination of performance of services.

71. CONTRACT TERM - RENEWAL In addition to any stated renewal periods in the Contract, any Contract or unit portion thereof let by the Commissioner may be extended by the Commissioner for an additional period(s) of up to one year with the written concurrence of the Contractor and Comptroller. Such extension may be exercised on a month to month basis or in other stated periods of time during the one year extension.

72. ADDITIONAL WARRANTIES Where Contractor, product manufacturer or service provider generally offers additional or more advantageous warranties than set forth below, Contractor shall offer or pass through any such warranties to Authorized Users. Contractor hereby warrants and represents:

a. Product Performance Contractor warrants and represents that Products delivered pursuant to this Contract conform to the manufacturer's specifications, performance standards and documentation, and the documentation fully describes the proper procedure for using the Products.

b. Title and Ownership Warranty Contractor warrants, represents and conveys (i) full ownership, clear title free of all liens, or (ii) the right to transfer or deliver perpetual license rights to any Products transferred to Authorized User under this Contract. Contractor shall be solely liable for any costs of acquisition associated therewith. Contractor fully indemnifies the Authorized User for any loss, damages or actions arising from a breach of said warranty without limitation.

c. Contractor Compliance Contractor represents and warrants to pay, at its sole expense, for all applicable permits, licenses, tariffs, tolls and fees to give all notices and comply with all laws, ordinances, rules and regulations of any governmental entity in conjunction with the performance of obligations under the Contract. Prior to award and during the Contract term and any renewals thereof, Contractor must establish to the satisfaction of the Commissioner that it meets or

exceeds all requirements of the Bid/Contract and any applicable laws, including but not limited to, permits, insurance coverage, licensing, proof of coverage for worker's compensation, and shall provide such proof as required by the Commissioner. Failure to do so may constitute grounds for the Commissioner to cancel or suspend this Contract, in whole or in part, or to take any other action deemed necessary by the Commissioner.

d. Product Warranty Unless recycled or recovered materials are available in accordance with the "Recycled or Recovered Materials" clause, Product offered shall be standard new equipment, current model or most recent release of regular stock product with all parts regularly used with the type of equipment offered; and no attachment or part has been substituted or applied contrary to the manufacturer's recommendations and standard practice.

Contractor further warrants and represents that components or deliverables specified and furnished by or through Contractor shall individually, and where specified and furnished as a system, be substantially uninterrupted or error-free in operation and guaranteed against faulty material and workmanship for the warranty period, or for a minimum of one (1) year from the date of acceptance, whichever is longer ("Project warranty period"). During the Project warranty period, defects in the materials or workmanship of components or deliverables specified and furnished by or through Contractor shall be repaired or replaced by Contractor at no cost or expense to the Authorized User. Contractor shall extend the Project warranty period for individual component(s), or for the System as a whole, as applicable, by the cumulative period(s) of time, after notification, during which an individual component or the System requires servicing or replacement (down time) or is in the possession of the Contractor, its agents, officers, Subcontractors, distributors, resellers or employees ("extended warranty").

Where Contractor, the Independent Software Vendor "ISV," or other third party manufacturer markets any Project Deliverable delivered by or through Contractor with a standard commercial warranty, such standard warranty shall be in addition to, and not relieve the Contractor from, Contractor's warranty obligations during the project warranty and extended warranty period(s). Where such standard commercial warranty covers all or some of the Project warranty or extended warranty period(s), Contractor shall be responsible for the coordination during the Project warranty or extended warranty period(s) with ISV or other third party manufacturer(s) for warranty repair or replacement of ISV or other third party manufacturer's Product.

Where Contractor, ISV or other third party manufacturer markets any Project Deliverable with a standard commercial warranty which goes beyond the Project warranty or extended warranty period(s), Contractor shall notify the Authorized User and pass through the manufacturer's standard commercial warranty to Authorized User at no additional charge; provided, however, that Contractor shall not be responsible for coordinating services under the third party extended warranty after expiration of the Project warranty and extended warranty period(s).

e. Replacement Parts Warranty If during the regular or extended warranty period's faults develop, the Contractor shall promptly repair or, upon demand, replace the defective unit or component part affected. All costs for labor and material and transportation incurred to repair or replace defective Product during the warranty period shall be borne solely by the Contractor, and the State or Authorized User shall in no event be liable or responsible therefor.

Any part of component replaced by the Contractor under the Contract warranty shall be replaced at no cost to the Authorized User and guaranteed for the greater of: a) the warranty period under paragraph (d) above; or b) if a separate warranty for that part or component is generally offered by the manufacturer, the standard commercial warranty period offered by the manufacturer for the individual part or component.

f. Virus Warranty The Contractor represents and warrants that Licensed Software contains no known viruses. Contractor is not responsible for viruses introduced at Licensee's site.

g. Date/Time Warranty Contractor warrants that Product(s) furnished pursuant to this Contract shall, when used in accordance with the Product documentation, be able to accurately process date/time data (including, but not limited to, calculating, comparing, and sequencing) transitions, including leap year calculations. Where a Contractor proposes or an acquisition requires that specific Products must perform as a package or system, this warranty shall apply to the Products as a system.

Where Contractor is providing ongoing services, including but not limited to: i) consulting, integration, code or data conversion, ii) maintenance or support services, iii) data entry or processing, or iv) contract administration services (e.g., billing, invoicing, claim processing), Contractor warrants that services shall be provided in an accurate and timely manner without interruption, failure or error due to the inaccuracy of Contractor's business operations in processing date/time data (including, but not limited to, calculating, comparing, and sequencing) various date/time transitions, including leap year calculations. Contractor shall be responsible for damages resulting from any delays, errors or untimely performance resulting therefrom, including but not limited to the failure or untimely performance of such services.

This Date/Time Warranty shall survive beyond termination or expiration of this contract through: a) ninety (90) days or b) the Contractor's or Product manufacturer/developer's stated date/time warranty term, whichever is longer. Nothing in this warranty statement shall be construed to limit any rights or remedies otherwise available under this Contract for breach of warranty.

h. Workmanship Warranty Contract warrants that all components or deliverables specified and furnished by or through Contractor under the Project Definition/Work Order meet the completion criteria set forth in the Project Definition/Work Order and any subsequent statement(s) of work, and that services will be provided in a workmanlike manner in accordance with industry standards.

i. Survival of Warranties All warranties contained in this Contract shall survive the termination of this Contract.

73. LEGAL COMPLIANCE Contractor represents and warrants that it shall secure all notices and comply with all laws, ordinances, rules and regulations of any governmental entity in conjunction with the performance of obligations under the Contract. Prior to award and during the Contract term and any renewals thereof, Contractor must establish to the satisfaction of the Commissioner that it meets or exceeds all requirements of the Bid and Contract and any applicable laws, including but not limited to, permits, licensing, and shall provide such proof as required by the Commissioner. Failure to comply or failure to provide proof may constitute grounds for the Commissioner to cancel or suspend the Contract, in whole or in part, or to take any other action deemed necessary by the Commissioner. Contractor also agrees to disclose information and provide affirmations and certifications to comply with Sections 139-j and 139-k of the State Finance Law.

74. INDEMNIFICATION Contractor shall be fully liable for the actions of its agents, employees, partners or Subcontractors and shall fully indemnify and save harmless the Authorized Users from suits, actions, damages and costs of every name and description relating to personal injury and damage to real or personal tangible property caused by any intentional act or negligence of Contractor, its agents, employees, partners or Subcontractors, without limitation; provided, however, that the Contractor shall not indemnify for that portion of any claim, loss or damage arising hereunder due to the negligent act or failure to act of the Authorized Users.

75. INDEMNIFICATION RELATING TO THIRD PARTY RIGHTS The Contractor will also indemnify and hold the Authorized Users harmless from and against any and all damages, expenses (including reasonable attorneys' fees), claims, judgments, liabilities and costs that may be finally assessed against the Authorized Users in any action for infringement of a United States Letter Patent, or of any copyright, trademark, trade secret or other third party proprietary right except to the extent such claims arise from the Authorized Users gross negligence or willful misconduct, provided that the State shall give Contractor: (i) prompt written notice of any action, claim or threat of infringement suit, or other suit, (ii) the opportunity to take over, settle or defend such action, claim or suit at Contractor's sole expense, and (iii) assistance in the defense of any such action at the expense of Contractor.

If usage shall be enjoined for any reason or if Contractor believes that it may be enjoined, Contractor shall have the right, at its own expense and sole discretion to take action in the following order of precedence: (i) to procure for the Authorized User the right to continue Usage (ii) to modify the service or Product so that Usage becomes non-infringing, and is of at least equal quality and performance; or (iii) to replace said service or Product or part(s) thereof, as applicable, with non-infringing service or Product of at least equal quality and performance. If the above remedies are not available, the parties shall terminate the Contract, in whole or in part as necessary and applicable, provided the Authorized User is given a refund for any amounts paid for the period during which Usage was not feasible.

The foregoing provisions as to protection from third party rights shall not apply to any infringement occasioned by modification by the Authorized User of any Product without Contractor's approval.

In the event that an action at law or in equity is commenced against the Authorized User arising out of a claim that the Authorized User's use of the service or Product under the Contract infringes any patent, copyright or proprietary right, and Contractor is of the opinion that the allegations in such action in whole or in part are not covered by the indemnification and defense provisions set forth in the Contract, Contractor shall immediately notify the Authorized User and the Office of the Attorney General in writing and shall specify to what extent Contractor believes it is obligated to defend and indemnify under the terms and conditions of the Contract. Contractor shall in such event protect the interests of the Authorized User and secure a continuance to permit the Authorized User to appear and defend its interests in cooperation with Contractor, as is appropriate, including any jurisdictional defenses the Authorized User may have. This constitutes the Authorized User's sole and exclusive remedy for patent infringement, or for infringement of any other third party proprietary right.

76. LIMITATION OF LIABILITY Except as otherwise set forth in the Indemnification Paragraphs above, the limit of liability shall be as follows:

a. Contractor's liability for any claim, loss or liability arising out of, or connected with the Products and services provided, and whether based upon default, or other liability such as breach of contract, warranty, negligence, misrepresentation or otherwise, shall in no case exceed direct damages in: (i) an amount equal to two (2) times the charges specified in the Purchase Order for the Products and services, or parts thereof forming the basis of the Authorized User's claim, (said amount not to exceed a total of twelve (12) months charges payable under the applicable Purchase Order) or (ii) one million dollars (\$1,000,000), whichever is greater.

b. The Authorized User may retain such monies from any amount due Contractor as may be necessary to satisfy any claim for damages, costs and the like asserted against the Authorized User unless Contractor at the time of the presentation of claim shall demonstrate to the Authorized User's satisfaction that sufficient monies are set aside by the Contractor in the form of a bond or through insurance coverage to cover associated damages and other costs.

c. Notwithstanding the above, neither the Contractor nor the Authorized User shall be liable for any consequential, indirect or special damages of any kind which may result directly or indirectly from such performance, including, without limitation, damages resulting from loss of use or loss of profit by the Authorized User, the Contractor, or by others.

77. INSURANCE Contractor shall secure and maintain insurance coverage as specified in the Bid Documents and shall promptly provide documentation of specified coverages to the Authorized User. If specified, the Contractor may be required to add the Authorized User as an additional insured.

THE FOLLOWING CLAUSES PERTAIN TO TECHNOLOGY & NEGOTIATED CONTRACTS

78. SOFTWARE LICENSE GRANT Where Product is acquired on a licensed basis the following shall constitute the license grant:

a. **License Scope** Licensee is granted a non-exclusive, perpetual license to use, execute, reproduce, display, perform, or merge the Product within its business enterprise in the United States up to the maximum licensed capacity stated on the Purchase Order. Product may be accessed, used, executed, reproduced, displayed or performed up to the capacity measured by the applicable licensing unit stated on the Purchase Order (i.e., payroll size, number of employees, CPU, MIPS, MSU, concurrent user, workstation). Licensee shall have the right to use and distribute modifications or customizations of the Product to and for use by any Authorized Users otherwise licensed to use the Product, provided that any modifications, however extensive, shall not diminish Licensor's proprietary title or interest. No license, right or interest in any trademark, trade name, or service mark is granted hereunder.

b. **License Term** The license term shall commence upon the License Effective Date, provided, however, that where an acceptance or trial period applies to the Product, the License Term shall be extended by the time period for testing, acceptance or trial.

c. **Licensed Documentation** If commercially available, Licensee shall have the option to require the Contractor to deliver, at Contractor's expense: (i) one (1) hard copy and one (1) master electronic copy of the Documentation in a mutually agreeable format; (ii) based on hard copy instructions for access by downloading from the Internet (iii) hard copies of the Product Documentation by type of license in the following amounts, unless otherwise mutually agreed:

- Individual/Named User License - one (1) copy per License
- Concurrent Users - 10 copies per site
- Processing Capacity - 10 copies per site

Software media must be in a format specified by the Authorized User, without requiring any type of conversion.

Contractor hereby grants to Licensee a perpetual license right to make, reproduce (including downloading electronic copies of the Product) and distribute, either electronically or otherwise, copies of Product Documentation as necessary to enjoy full use of the Product in accordance with the terms of license.

d. Product Technical Support & Maintenance Licensee shall have the option of electing the Product technical support and maintenance ("maintenance") set forth in the Contract by giving written notice to Contractor any time during the Centralized Contract term. Maintenance term(s) and any renewal(s) thereof are independent of the expiration of the Centralized Contract term and will not automatically renew.

Maintenance shall include, at a minimum, (i) the provision of error corrections, updates, revisions, fixes, upgrade and new releases to Licensee, and (ii) Help Desk assistance with locally accessible "800" or toll free, local telephone service, or alternatively on-line Help Desk accessibility. Contractor shall maintain the Products so as to provide Licensee with the ability to utilize the Products in accordance with the Product documentation without significant functional downtime to its ongoing business operations during the maintenance term.

Authorized User shall not be required to purchase maintenance for use of Product, and may discontinue maintenance at the end of any current maintenance term upon notice to Contractor. In the event that Authorized User does not initially acquire or discontinues maintenance of licensed Product, it may, at any time thereafter, reinstate maintenance for Product without any additional penalties or other charges, by paying Contractor the amount which would have been due under the Contract for the period of time that such maintenance had lapsed, at then current NYS net maintenance rates.

e. Permitted License Transfers As Licensee's business operations may be altered, expanded or diminished, licenses granted hereunder may be transferred or combined for use at an alternative or consolidated site not originally specified in the license, including transfers between Agencies ("permitted license transfers"). Licensee(s) do not have to obtain the approval of Contractor for permitted license transfers, but must give thirty (30) days prior written notice to Contractor of such move(s) and certify in writing that the Product is not in use at the prior site. There shall be no additional license or other transfer fees due Contractor, provided that: i) the maximum capacity of the consolidated machine is equal to the combined individual license capacity of all licenses running at the consolidated or transferred site (e.g., named users, seats, or MIPS); or ii) if the maximum capacity of the consolidated machine is greater than the individual license capacity being transferred, a logical or physical partition or other means of restricting access will be maintained within the computer system so as to restrict use and access to the Product to that unit of licensed capacity solely dedicated to beneficial use for Licensee. In the event that the maximum capacity of the consolidated machine is greater than the combined individual license capacity of all licenses running at the consolidated or transferred site, and a logical or physical partition or other means of restricting use is not available, the fees due Contractor shall not exceed the fees otherwise payable for a single license for the upgrade capacity.

f. Restricted Use By Outsourcers / Facilities Management, Service Bureaus / or Other Third Parties Outsourcers, facilities management or service bureaus retained by Licensee shall have the right to use the Product to maintain Licensee's business operations, including data processing, for the time period that they are engaged in such activities, provided that: 1) Licensee gives notice to Contractor of such party, site of intended use of the Product, and means of access; and 2) such party has executed, or agrees to execute, the Product manufacturer's standard nondisclosure or restricted use agreement which executed agreement shall be accepted by the Contractor ("Non-Disclosure Agreement"); and 3) if such party is engaged in the business of facility management, outsourcing, service bureau or other services, such third party will maintain a logical or physical partition within its computer system so as to restrict use and access to the program to that portion solely dedicated to beneficial use for Licensee. In no event shall Licensee assume any liability for third party's compliance with the terms of the Non-Disclosure Agreement, nor shall the Non-Disclosure Agreement create or impose any liabilities on the State or Licensee.

Any third party with whom a Licensee has a relationship for a state function or business operation, shall have the temporary right to use Product (e.g., JAVA Applets), provided that such use shall be limited to the time period during which the third party is using the Product for the function or business activity.

g. Archival Back-Up and Disaster Recovery Licensee may use and copy the Product and related Documentation in connection with: i) reproducing a reasonable number of copies of the Product for archival backup and disaster recovery procedures in the event of destruction or corruption of the Product or disasters or emergencies which require Licensee to restore backup(s) or to initiate disaster recovery procedures for its platform or operating systems; ii) reproducing a reasonable number of copies of the Product and related Documentation for cold site storage. "Cold Site" storage shall be defined as a restorable back-up copy of the Product not to be installed until and after the declaration by the Licensee of a disaster; iii) reproducing a back-up copy of the Product to run for a reasonable period of time in conjunction with a documented consolidation or transfer otherwise allowed herein. "Disaster Recovery" shall be defined as the installation and storage of Product in ready-to-execute, back-up computer systems prior to disaster or breakdown which is not used for active production or development.

h. Confidentiality Restrictions The Product is a trade secret, copyrighted and proprietary product. Licensee and its employees will keep the Product strictly confidential, and Licensee will not disclose or otherwise distribute or reproduce any Product to anyone other than as authorized under the terms of Contract. Licensee will not remove or destroy any proprietary markings of Contractor.

i. Restricted Use by Licensee Except as expressly authorized by the terms of license, Licensee shall not:

- (i) Copy the Product;
- (ii) Cause or permit reverse compilation or reverse assembly of all or any portion of the Product;
- (iii) Export the Licensed Software in violation of any U.S. Department of Commerce export administration regulations.

79. PRODUCT ACCEPTANCE Unless otherwise provided by mutual agreement of the Authorized User and the Contractor, Authorized User(s) shall have thirty (30) days from the date of delivery to accept hardware products and sixty (60) days from the date of delivery to accept all other Product. Where the Contractor is responsible for installation, acceptance shall be from completion of installation.

Failure to provide notice of acceptance or rejection or a deficiency statement to the Contractor by the end of the period provided for under this clause constitutes acceptance by the Authorized User(s) as of the expiration of that period. The License Term shall be extended by the time periods allowed for trial use, testing and acceptance unless the Commissioner or Authorized User agrees to accept the Product at completion of trial use.

Unless otherwise provided by mutual agreement of the Authorized User and the Contractor, Authorized User shall have the option to run testing on the Product prior to acceptance, such tests and data sets to be specified by User. Where using its own data or tests, Authorized User must have the tests or representative set of data available upon delivery. This demonstration will take the form of a documented installation test, capable of observation by the Authorized User, and shall be made part of the Contractor's standard documentation. The test data shall remain accessible to the Authorized User after completion of the test.

In the event that the documented installation test cannot be completed successfully within the specified acceptance period, and the Contractor or Product is responsible for the delay, Authorized User shall have the option to cancel the order in whole or in part, or to extend the testing period for an additional thirty (30) day increment. Authorized User shall notify Contractor of acceptance upon successful completion of the documented installation test. Such cancellation shall not give rise to any cause of action against the Authorized User for damages, loss of profits, expenses, or other remuneration of any kind.

If the Authorized User elects to provide a deficiency statement specifying how the Product fails to meet the specifications within the testing period, Contractor shall have thirty (30) days to correct the deficiency, and the Authorized User shall have an additional sixty (60) days to evaluate the Product as provided herein. If the Product does not meet the specifications at the end of the extended testing period, Authorized User, upon prior written notice to Contractor, may then reject the Product and return all defective Product to Contractor, and Contractor shall refund any monies paid by the Authorized User to Contractor therefor. Costs and liabilities associated with a failure of the Product to perform in accordance with the functionality tests or product specifications during the acceptance period shall be borne fully by Contractor to the extent that said costs or liabilities shall not have been caused by negligent or willful acts or omissions of the Authorized User's agents or employees. Said costs shall be limited to the amounts set forth in the Limitation of Liability Clause for any liability for costs incurred at the direction or recommendation of Contractor.

80. AUDIT OF LICENSED PRODUCT USAGE Contractor shall have the right to periodically audit, no more than annually, at Contractor's expense, use of licensed Product at any site where a copy of the Product resides provided that: (i) Contractor gives Licensee(s) at least thirty (30) days advance written notice, (ii) such audit is conducted during such party's normal business hours, (iii) the audit is conducted by an independent auditor chosen on mutual agreement of the parties. Contractor shall recommend a minimum of three (3) auditing/accounting firms from which the Licensee will select one (1). In no case shall the Business Software Alliance (BSA), Software Publishers Association (SPA), Software and Industry Information Association (SIIA) or Federation Against Software Theft (FAST) be used directly or indirectly to conduct audits, or be recommended by Contractor; (iv) Contractor and Licensee are each entitled to designate a representative who shall be entitled to participate, and who shall mutually agree on audit format, and simultaneously review all information obtained by the audit. Such representatives also shall be entitled to copies of all reports, data or information obtained from the

audit; and (v) if the audit shows that such party is not in compliance, Licensee shall be required to purchase additional licenses or capacities necessary to bring it into compliance and shall pay for the unlicensed capacity at the NYS Net Price in effect at time of audit, or if none, then at the Contractor's U.S. Commercial list price. Once such additional licenses or capacities are purchased, Licensee shall be deemed to have been in compliance retroactively, and Licensee shall have no further liability of any kind for the unauthorized use of the software.

81. OWNERSHIP/TITLE TO PROJECT DELIVERABLES

a. Definitions

(i) For purposes of this paragraph, "Products." A deliverable furnished under this Contract by or through Contractor, including existing and custom Products, including, but not limited to: a) components of the hardware environment, b) printed materials (including but not limited to training manuals, system and user documentation, reports, drawings), whether printed in hard copy or maintained on diskette, CD, DVD or other electronic media c) third party software, d) modifications, customizations, custom programs, program listings, programming tools, data, modules, components, and e) any properties embodied therein, whether in tangible or intangible form (including but not limited to utilities, interfaces, templates, subroutines, algorithms, formulas, source code, object code).

(ii) For purposes of this paragraph, "Existing Products." Tangible Products and intangible licensed Products that exist prior to the commencement of work under the Contract. Contractor bears the burden of proving that a particular product was in existence prior to the commencement of the Project.

(iii) For purposes of this paragraph, "Custom Products." Products, preliminary, final or otherwise, which are created or developed by Contractor, its Subcontractors, partners, employees or agents for Authorized User under the Contract.

b. Title to Project Deliverables Contractor acknowledges that it is commissioned by the Authorized User to perform the services detailed in the Purchase Order. Unless otherwise specified in writing in the Bid or Purchase Order, the Authorized User shall have ownership and license rights as follows:

(i) Existing Products:

1. Hardware - Title and ownership of Existing Hardware Product shall pass to Authorized User upon Acceptance.

2. Software - Title and ownership to Existing Software Product(s) delivered by Contractor under the Contract that is normally commercially distributed on a license basis by the Contractor or other independent software vendor proprietary owner ("Existing Licensed Product"), whether or not embedded in, delivered or operating in conjunction with hardware or Custom Products, shall remain with Contractor or the proprietary owner of other independent software vendor(s) (ISV). Effective upon acceptance, such Product shall be licensed to Authorized User in accordance with the Contractor or ISV owner's standard license agreement, provided, however, that such standard license, must, at a minimum: (a) grant Authorized User a non-exclusive, perpetual license to use, execute, reproduce, display, perform, adapt (unless Contractor advises Authorized User as part of Contractor's proposal that adaptation will violate existing agreements or statutes and Contractor demonstrates such to the Authorized User's satisfaction) and distribute Existing Licensed Product to the Authorized User up to the license capacity stated in the Purchase Order or work order with all license rights necessary to fully effect the general business purpose(s) stated in the Bid or Authorized User's Purchase Order or work order, including the financing assignment rights set forth in paragraph (c) below; and (b) recognize the State of New York as the licensee where the Authorized User is a state agency,

department, board, commission, office or institution. Where these rights are not otherwise covered by the ISV's owner's standard license agreement, the Contractor shall be responsible for obtaining these rights at its sole cost and expense. The Authorized User shall reproduce all copyright notices and any other legend of ownership on any copies authorized under this paragraph.

(ii.) **Custom Products:** Effective upon creation of Custom Products, Contractor hereby conveys, assigns and transfers to Authorized User the sole and exclusive rights, title and interest in Custom Product(s), whether preliminary, final or otherwise, including all trademark and copyrights. Contractor hereby agrees to take all necessary and appropriate steps to ensure that the Custom Products are protected against unauthorized copying, reproduction and marketing by or through Contractor, its agents, employees, or Subcontractors. Nothing herein shall preclude the Contractor from otherwise using the related or underlying general knowledge, skills, ideas, concepts, techniques and experience developed under a Purchase Order, project definition or work order in the course of Contractor's business. Authorized User may, by providing written notice thereof to the Contractor, elect in the alternative to take a non-exclusive perpetual license to Custom Products in lieu of Authorized User taking exclusive ownership and title to such Products. In such case, Licensee on behalf of all Authorized Users shall be granted a non-exclusive perpetual license to use, execute, reproduce, display, perform, adapt and distribute Custom Product as necessary to fully effect the general business purpose(s) as stated in paragraph (b)(i)(2), above.

c. **Transfers or Assignments to a Third Party Financing Agent** It is understood and agreed by the parties that a condition precedent to the consummation of the purchase (s) under the Contract may be the obtaining of acceptable third party financing by the Authorized User. The Authorized User shall make the sole determination of the acceptability of any financing proposal. The Authorized User will make all reasonable efforts to obtain such financing, but makes no representation that such financing has been obtained as of the date of Bid receipt. Where financing is used, Authorized User may assign or transfer its rights in Licensed Products (existing or custom) to a third party financing entity or trustee ("Trustee") as collateral where required by the terms of the financing agreement. Trustee's sole rights with respect to transferability or use of Licensed Products shall be to exclusively sublicense to Authorized User all of its Licensee's rights under the terms and conditions of the License Agreement; provided, further, however, in the event of any termination or expiration of such sublicense by reason of payment in full, all of Trustee's rights in such Licensed Product shall terminate immediately and Authorized User's prior rights to such Existing Licensed Product shall be revived.

d. **Sale or License of Custom Products Involving Tax-Exempt Financing (i.e., Certificates of Participation - COPS)** The Authorized User's sale or other transfer of Custom Products which were acquired by the Authorized User using third party, tax-exempt financing may not occur until such Custom Products are, or become, useable. In the event that the Contractor wishes to obtain ownership rights to Custom Product(s), the sale or other transfer shall be at fair market value determined at the time of such sale or other transfer, and must be pursuant to a separate written agreement in a form acceptable to the Authorized User which complies with the terms of this paragraph.

e. **Contractor's Obligation with Regard to ISV (Third Party) Product** Where Contractor furnishes Existing Licensed Product(s) as a Project Deliverable, and sufficient rights necessary to effect the purposes of this section are not otherwise provided in the Contractor or ISV's standard license agreement, Contractor shall be responsible for obtaining from the ISV third party proprietary owner/developer the rights set forth

herein to the benefit of the Authorized User at Contractor's sole cost and expense.

82. PROOF OF LICENSE The Contractor must provide to each Licensee who places a Purchase Order either: (i) the Product developer's certified License Confirmation Certificates in the name of such Licensee; or (ii) a written confirmation from the Proprietary owner accepting Product invoice as proof of license. Contractor shall submit a sample certificate, or alternatively such written confirmation from the proprietary developer. Such certificates must be in a form acceptable to the Licensee.

83. PRODUCT VERSION Purchase Orders shall be deemed to reference Manufacturer's most recently released model or version of the Product at time of order, unless an earlier model or version is specifically requested in writing by Authorized User and Contractor is willing to provide such version.

84. CHANGES TO PRODUCT OR SERVICE OFFERINGS

a. **Product or Service Discontinuance** Where Contractor is the Product Manufacturer/Developer, and Contractor publicly announces to all U.S. customers ("date of notice") that a Product is being withdrawn from the U.S. market or that maintenance service or technical support provided by Contractor ("withdrawn support") is no longer going to be offered, Contractor shall be required to: (i) notify the Commissioner, each Licensee and each Authorized User then under contract for maintenance or technical support in writing of the intended discontinuance; and (ii) continue to offer Product or withdrawn support upon the Contract terms previously offered for the greater of: a) the best terms offered by Contractor to any other customer, or b) not less than twelve (12) months from the date of notice; and (iii) at Authorized User's option, provided that the Authorized User is under contract for maintenance on the date of notice, either: provide the Authorized User with a Product replacement or migration path with at least equivalent functionality at no additional charge to enable Authorized User to continue use and maintenance of the Product.

In the event that the Contractor is not the Product Manufacturer, Contractor shall be required to: (i) provide the notice required under the paragraph above, to the entities described within five (5) business days of Contractor receiving notice from the Product Manufacturer, and (ii) include in such notice the period of time from the date of notice that the Product Manufacturer will continue to provide Product or withdraw support.

The provisions of this subdivision (a) shall not apply or eliminate Contractor's obligations where withdrawn support is being provided by an independent Subcontractor. In the event that such Subcontractor ceases to provide service, Contractor shall be responsible for subcontracting such service, subject to state approval, to an alternate Subcontractor.

b. **Product or Service Re-Bundling** In the event that Contractor is the Product manufacturer and publicly announces to all U.S. customers ("date of notice") that a Product or maintenance or technical support offering is being re-bundled in a different manner from the structure or licensing model of the prior U.S. commercial offering, Contractor shall be required to: (i) notify the State and each Authorized User in writing of the intended change; (ii) continue to provide Product or withdrawn support upon the same terms and conditions as previously offered on the then-current NYS Contract for the greater of: a) the best terms offered by Contractor to any other customer, or b) not less than twelve (12) months from the date of notice; and (iii) shall submit the proposed rebundling change to the Commissioner for approval prior to its becoming effective for the remainder of the Contract term. The

provisions of this section do not apply if the Contractor is not the Product manufacturer.

85. NO HARDSTOP/PASSIVE LICENSE MONITORING

Unless an Authorized User is otherwise specifically advised to the contrary in writing at the time of order and prior to purchase, Contractor hereby warrants and represents that the Product and all Upgrades do not and will not contain any computer code that would disable the Product or Upgrades or impair in any way its operation based on the elapsing of a period of time, exceeding an authorized number of copies, advancement to a particular date or other numeral, or other similar self-destruct mechanisms (sometimes referred to as “time bombs,” “time locks,” or “drop dead” devices) or that would permit Contractor to access the Product to cause such disablement or impairment (sometimes referred to as a “trap door” device). Contractor agrees that in the event of a breach or alleged breach of this provision that Authorized User shall not have an adequate remedy at law, including monetary damages, and that Authorized User shall consequently be entitled to seek a temporary restraining order, injunction, or other form of equitable relief against the continuance of such breach, in addition to any and all remedies to which Authorized User shall be entitled.

86. SOURCE CODE ESCROW FOR LICENSED PRODUCT

If Source Code or Source Code escrow is offered by either Contractor or Product manufacturer or developer to any other commercial customers, Contractor shall either: (i) provide Licensee with the Source Code for the Product; or (ii) place the Source Code in a third party escrow arrangement with a designated escrow agent who shall be named and identified to the State, and who shall be directed to release the deposited Source Code in accordance with a standard escrow agreement acceptable to the State; or (iii) will certify to the State that the Product manufacturer/developer has named the State, acting by and through the Authorized User, and the Licensee, as a named beneficiary of an established escrow arrangement with its designated escrow agent who shall be named and identified to the State and Licensee, and who shall be directed to release the deposited Source Code in accordance with the terms of escrow. Source Code, as well as any corrections or enhancements to such source code, shall be updated for each new release of the Product in the same manner as provided above and such updating of escrow shall be certified to the State in writing. Contractor shall identify the escrow agent upon commencement of the Contract term and shall certify annually that the escrow remains in effect in compliance with the terms of this paragraph.

The State may release the Source Code to Licensees under this Contract who have licensed Product or obtained services, who may use such copy of the Source Code to maintain the Product.

I N D E X

	<u>Paragraph</u>		<u>Paragraph</u>
<u>A</u>	<u>No.</u>	<u>M</u>	<u>No.</u>
Additional Warranties	72	Modification of Contract Terms	40
Advertising Results	20		
Applicability	1	<u>N</u>	
Assignment	56	No Hardstop/Passive License Monitoring	85
Assignment of Claim	66		
Audit of Licensed Product Usage	80	<u>O</u>	
		On-Site Storage	54
<u>B</u>		Ownership/Title to Project Deliverables	81
Bid Contents	12		
Bid Evaluation	29	<u>P</u>	
Bid Opening	7	Participation in Centralized Contracts	39
Bid Submission	8	Performance and Responsibility Qualifications	34
		Performance/Bid Bond	58
<u>C</u>		Prevailing Wage Rates Public Works	
Changes to Product or Service Offerings	84	& Building Services Contracts	17
Clarification/Revisions	31	Pricing	24
Confidential/Trade Secret Materials	14	Procurement Card	27
Contract Creation/Execution	38	Product Acceptance	79
Contract Term - Renewal	71	Product Version	83
Cooperation with Third Parties	70	Prompt Payment Discounts	32
		Proof of License	82
<u>D</u>		Purchase Orders	44
Default - Authorized User	63		
Definitions	5	<u>Q</u>	
Disqualification for Past Performance	35	Quantity Changes Prior to Award	36
Drawings	25		
		<u>R</u>	
<u>E</u>		Release of Bid Evaluation Materials	15
Emergency Contracts	43	Remanufactured, Recycled, Recyclable or	
Employees/Subcontractors/Agents	55	Recovered Materials	22
Equivalent or Identical Bids	33	Remedies for Breach	65
Ethics Compliance	3	Repaired or Replaced Product/Components	53
Expenses Prior to Contract Execution	19		
Extraneous Terms	13	<u>S</u>	
		Savings/Force Majeure	61
<u>F</u>		Scope Changes	41
Freedom of Information Law	16	Security	69
		Site Inspection	26
<u>G</u>		Software License Grant	78
Governing Law	2	Source Code Escrow for Licensed Product	86
		Subcontractors and Suppliers	57
<u>I</u>		Suspension of Work	59
Indemnification	74		
Indemnification Relating to Third Party Rights	75	<u>T</u>	
Independent Contractor	68	Taxes	18
Installation	52	Termination	60
Insurance	77	Timeframe for Offers	37
International Bidding	6	Title and Risk of Loss	48
		Toxic Substances	67
<u>L</u>			
Legal Compliance	73	<u>W</u>	
Limitation of Liability	76		

Appendix C

MWBE Reports

This Page Intentionally Blank

MWBE SUBCONTRACTOR UTILIZATION QUARTERLY REPORT

This report is to be submitted to DCJS quarterly during the life of this contract to report the actual payments made to all certified minority or women-owned subcontractors utilized for this project. Complete and mail to NYS Division of Criminal Justice Services, Financial Services, 4 Tower Place, Albany, NY 12203 or email completed form as an attachment to Procurement.officer@dcjs.state.ny.us.

Contractor	Contract No.	Place an X in the box for the quarter you are reporting on. ☐ 1 st Quarter (Apr 1-June 30) ☐ 2 nd Quarter (July 1 – Sept 30) ☐ 3 rd Quarter (Sept 1 – Dec 31) ☐ 4 th Quarter (Jan 1 – Mar31)
Federal ID#	Project Name	
Contact Name	Contract Start Date	
Contact Email Address	Contract End Date	
Contact Phone#	Contract Amount	

Subcontractor Name	Federal ID Number	Total Subcontractor Contract Amount		Payments this Quarter		Previous Payments		Total Payments Made to Date	
		MBE	WBE	MBE	WBE	MBE	WBE	MBE	WBE
TOTAL		0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

Signature	Date
(Printed Name)	

WORK FORCE EMPLOYMENT UTILIZATION

Contract No.:	Reporting Entity: ☐ Contractor ☐ Subcontractor	Reporting Period: ☐ January 1, 20__ - March 31, 20__ ☐ April 1, 20__ - June 30, 20__ ☐ July 1, 20__ - September 30, 20__ ☐ October 1, 20__ - December 31, 20__
Contractor's Name:		
Contractor's Address:	Report includes: ☐ Work force to be utilized on this contract ☐ Contractor/Subcontractor's total work force	

Enter the total number of employees in each classification in each of the EEO-Job Categories identified.

EEO-Job Category	Work force by Gender		Race/Ethnic Identification						Disabled		Veteran	
	Total Work force	Male (M)	Female (F)	White (M) (F)	Black (M) (F)	Hispanic (M) (F)	Asian (M) (F)	Native American (M) (F)	(M)	(F)	(M)	(F)
Officials/Administrators												
Professionals												
Technicians												
Sales Workers												
Office/Clerical												
Craft Workers												
Laborers												
Service Workers												
Temporary /Apprentices												
Totals												

PREPARED BY (Signature):	TELEPHONE NO.:	DATE:
NAME AND TITLE OF PREPARER (Print or Type):	EMAIL ADDRESS:	
Submit completed form to: NYS (add Agency name) M/WBE 102 (Revised 11/08)		

General Instructions: The work force utilization (M/WBE 102) is to be submitted on a quarterly basis during the life of the contract to report the actual work force utilized in the performance of the contract broken down by the specified categories. When the work force utilized in the performance of the contract can be separated out from the contractor's and/or subcontractor's total work force, the contractor and/or subcontractor shall submit a Utilization Report of the work force utilized on the contract. When the work force to be utilized on the contract cannot be separated out from the contractor's and/or subcontractor's total work force, information on the total work force shall be included in the Utilization Report. Utilization reports are to be completed for the quarters ended 3/31, 6/30, 9/30 and 12/31 and submitted to the M/WBE Program Management Unit within 15 days of the end of each quarter. If there are no changes to the work force utilized on the contract during the reporting period, the contractor can submit a copy of the previously submitted report indicating no change with the date and reporting period updated.

Instructions for completing:

1. Enter the number of the contract that this report applies to along with the name and address of the Contractor preparing the report.
2. Check off the appropriate box to indicate if the entity completing the report is the contractor or a subcontractor.
3. Check off the box that corresponds to the reporting period for this report.
4. Check off the appropriate box to indicate if the work force being reported is just for the contract or the Contractor's total work force.
5. Enter the total work force by EEO job category.
6. Break down the total work force by gender and enter under the heading 'Work force by Gender'
7. Break down the total work force by race/ethnic background and enter under the heading 'Work force by Race/Ethnic Identification'. Contact the M/WBE Program Management Unit at (518) 474-5513 if you have any questions.
8. Enter information on any disabled or veteran employees included in the work force under the appropriate heading.
9. Enter the name, title, phone number and email address for the person completing the form. Sign and date the form in the designated boxes.

RACE/ETHNIC IDENTIFICATION

Race/ethnic designations as used by the Equal Employment Opportunity Commission do not denote scientific definitions of anthropological origins. For the purposes of this report, an employee may be included in the group to which he or she appears to belong, identifies with, or is regarded in the community as belonging. However, no person should be counted in more than one race/ethnic group. The race/ethnic categories for this survey are:

- **WHITE** (Not of Hispanic origin) All persons having origins in any of the original peoples of Europe, North Africa, or the Middle East.
- **BLACK** a person, not of Hispanic origin, who has origins in any of the black racial groups of the original peoples of Africa.
- **HISPANIC** a person of Mexican, Puerto Rican, Cuban, Central or South American or other Spanish culture or origin, regardless of race.
- **ASIAN & PACIFIC ISLANDER** a person having origins in any of the original peoples of the Far East, Southeast Asia, the Indian subcontinent or the Pacific Islands.
- **NATIVE INDIAN (NATIVE AMERICAN/ALASKAN NATIVE)** a person having origins in any of the original peoples of North America, and who maintains cultural identification through tribal affiliation or community recognition.
- **OTHER CATEGORIES**

DISABLED INDIVIDUAL	any person who:	- has a physical or mental impairment that substantially limits one or more major life activity(ies)
		- has a record of such an impairment; or
		- is regarded as having such an impairment.
- **VIETNAM ERA VETERAN GENDER**

Male	or	Female

a veteran who served at any time between and including January 1, 1963 and May 7, 1975.

REQUEST FOR WAIVER FORM

INSTRUCTIONS: SEE PAGE 2 OF THIS ATTACHMENT FOR REQUIREMENTS AND DOCUMENT SUBMISSION INSTRUCTIONS.			
Offerer/Contractor Name:		Federal Identification No.:	
Address:		Solicitation/Contract No.:	
City, State, Zip Code:		MBE %	WBE %
By submitting this form and the required information, the offerer/contractor certifies that every Good Faith Effort has been taken to promote M/WBE participation pursuant to the M/WBE requirements set forth under the contract.			
Contractor is requesting a:			
1. ☐ MBE Waiver – A waiver of the MBE Goal for this procurement is requested. ☐ Total ☐ Partial 2. ☐ WBE Waiver – A waiver of the WBE Goal for this procurement is requested. ☐ Total ☐ Partial 3. ☐ Waiver Pending ESD Certification – (Check here if subcontractors or suppliers of Contractor are not certified M/WBE, but an application for certification has been filed with Empire State Development.) Date of such filing with Empire State Development: _____			
PREPARED BY (Signature):		Date:	
SUBMISSION OF THIS FORM CONSTITUTES THE OFFERER/CONTRACTOR'S ACKNOWLEDGEMENT AND AGREEMENT TO COMPLY WITH THE M/WBE REQUIREMENTS SET FORTH UNDER NYS EXECUTIVE LAW, ARTICLE 15-A AND 5 NYCRR PART 143. FAILURE TO SUBMIT COMPLETE AND ACCURATE INFORMATION MAY RESULT IN A FINDING OF NONCOMPLIANCE AND/OR TERMINATION OF THE CONTRACT.		Telephone Number:	
Name and Title of Preparer (Printed or Typed):		Email Address:	
***** FOR M/WBE USE ONLY *****			
REVIEWED BY:		DATE:	
Submit with the bid or proposal or if submitting after award submit to:		Waiver Granted: ☐ YES MBE: ☐ WBE: ☐ ☐ Total Waiver ☐ Partial Waiver ☐ ESD Certification Waiver ☐ *Conditional ☐ Notice of Deficiency Issued _____ *Comments:	

REQUIREMENTS AND DOCUMENT SUBMISSION INSTRUCTIONS

When completing the Request for Waiver Form please check all boxes that apply. To be considered, the Request for Waiver Form must be accompanied by documentation for items 1 – 11, as listed below. If box # 3 has been checked above, please see item 11. Copies of the following information and all relevant supporting documentation must be submitted along with the request:

1. A statement setting forth your basis for requesting a partial or total waiver.
2. The names of general circulation, trade association, and M/WBE-oriented publications in which you solicited certified M/WBEs for the purposes of complying with your participation goals.
3. A list identifying the date(s) that all solicitations for certified M/WBE participation were published in any of the above publications.
4. A list of all certified M/WBEs appearing in the NYS Directory of Certified Firms that were solicited for purposes of complying with your certified M/WBE participation levels.
5. Copies of notices, dates of contact, letters, and other correspondence as proof that solicitations were made in writing and copies of such solicitations, or a sample copy of the solicitation if an identical solicitation was made to all certified M/WBEs.
6. Provide copies of responses made by certified M/WBEs to your solicitations.
7. Provide a description of any contract documents, plans, or specifications made available to certified M/WBEs for purposes of soliciting their bids and the date and manner in which these documents were made available.
8. Provide documentation of any negotiations between you, the Offerer/Contractor, and the M/WBEs undertaken for purposes of complying with the certified M/WBE participation goals.
9. Provide any other information you deem relevant which may help us in evaluating your request for a waiver.
10. Provide the name, title, address, telephone number, and email address of offerer/contractor's representative authorized to discuss and negotiate this waiver request.
11. Copy of notice of application receipt issued by Empire State Development (ESD).

Note:

Unless a Total Waiver has been granted, the Offerer/Contractor will be required to submit all reports and documents pursuant to the provisions set forth in the Contract, as deemed appropriate by AGENCY, to determine M/WBE compliance.

This Page Intentionally Blank

Appendix D

Criminal Justice Information Services (CJIS) Security Policy

This Page Intentionally Blank

U. S. Department of Justice

Federal Bureau of Investigation

Criminal Justice Information Services Division



Criminal Justice Information Services (CJIS) Security Policy

Version 5.3

8/4/2014

CJISD-ITS-DOC-08140-5.3



Prepared by:
CJIS Information Security Officer

Approved by:
CJIS Advisory Policy Board

EXECUTIVE SUMMARY

Law enforcement needs timely and secure access to services that provide data wherever and whenever for stopping and reducing crime. In response to these needs, the Advisory Policy Board (APB) recommended to the Federal Bureau of Investigation (FBI) that the Criminal Justice Information Services (CJIS) Division authorize the expansion of the existing security management structure in 1998. Administered through a shared management philosophy, the CJIS Security Policy contains information security requirements, guidelines, and agreements reflecting the will of law enforcement and criminal justice agencies for protecting the sources, transmission, storage, and generation of Criminal Justice Information (CJI). The Federal Information Security Management Act of 2002 provides further legal basis for the APB approved management, operational, and technical security requirements mandated to protect CJI and by extension the hardware, software and infrastructure required to enable the services provided by the criminal justice community.

The essential premise of the CJIS Security Policy is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CJIS Security Policy provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. This Policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information.

The CJIS Security Policy integrates presidential directives, federal laws, FBI directives and the criminal justice community's APB decisions along with nationally recognized guidance from the National Institute of Standards and Technology. The Policy is presented at both strategic and tactical levels and is periodically updated to reflect the security requirements of evolving business models. The Policy features modular sections enabling more frequent updates to address emerging threats and new security measures. The provided security criteria assists agencies with designing and implementing systems to meet a uniform level of risk and security protection while enabling agencies the latitude to institute more stringent security requirements and controls based on their business model and local needs.

The CJIS Security Policy strengthens the partnership between the FBI and CJIS Systems Agencies (CSA), including, in those states with separate authorities, the State Identification Bureaus (SIB). Further, as use of criminal history record information for noncriminal justice purposes continues to expand, the CJIS Security Policy becomes increasingly important in guiding the National Crime Prevention and Privacy Compact Council and State Compact Officers in the secure exchange of criminal justice records.

The Policy describes the vision and captures the security concepts that set the policies, protections, roles, and responsibilities with minimal impact from changes in technology. The Policy empowers CSAs with the insight and ability to tune their security programs according to their needs, budgets, and resource constraints while remaining compliant with the baseline level of security set forth in this Policy. The CJIS Security Policy provides a secure framework of laws, standards, and elements of published and vetted policies for accomplishing the mission across the broad spectrum of the criminal justice and noncriminal justice communities.

CHANGE MANAGEMENT

Revision	Change Description	Created/Changed by	Date	Approved By
5.0	Policy Rewrite	Security Policy Working Group	02/09/2011	See Signature Page
5.1	Incorporate Calendar Year 2011 APB approved changes and administrative changes	CJIS ISO Program Office	07/13/2012	APB & Compact Council
5.2	Incorporate Calendar Year 2012 APB approved changes and administrative changes	CJIS ISO Program Office	08/09/2013	APB & Compact Council
5.3	Incorporate Calendar Year 2013 APB approved changes and administrative changes	CJIS ISO Program Office	08/04/2014	APB & Compact Council

SUMMARY OF CHANGES

Version 5.3

APB Approved Changes

1. Section 5.3 Policy Area 3: Incident Response: added reference to new Section 5.13.5, Fall 2013, APB11, SA6, Future CSP for Mobile Devices.
2. Section 5.4 Policy Area 4: Auditing and Accountability: added reference to new Section 5.13.6, Fall 2013, APB11, SA6, Future CSP for Mobile Devices.
3. Section 5.5 Policy Area 5: Access Control: added reference to new Section 5.13.7, APB approved change, Fall 2013, APB11, SA6, Future CSP for Mobile Devices.
4. Section 5.5.5 Session Lock: added language for receive only terminals (ROT), Spring 2013, APB12, SA1, add ROT language.
5. Section 5.5.6.1 Personally Owned Information Systems: modified language and requirements for bring your own device(s) (BYOD), Fall 2013, APB11, SA6, Future CSP for Mobile Devices.
6. Section 5.5.7 Wireless Access Restrictions: moved to Section 5.13, Fall 2013, APB11, SA6, Future CSP for Mobile Devices.
7. Section 5.6.2.1 Standard Authenticators: modified language, Fall 2013, APB11, SA6, Future CSP for Mobile Devices.
8. Section 5.6.2.1.2 Personal Identification Number (PIN): added language from Appendix G-5 PIN, Fall 2013, APB11, SA6, Future CSP for Mobile Devices.
9. Section 5.6.2.2.1 Advance Authentication Policy and Rationale: removed Interim Compliance language, Spring 2013, APB12, SA5, AA exemption for police vehicles.
10. Section 5.6.2.2.1 Advance Authentication Policy and Rationale: added language for compensating controls, Spring 2013, APB12, SA8, compensating controls for AA on smartphones.
11. Section 5.6.2.2.1 Advance Authentication Policy and Rationale: added language for indirect access, Fall 2013, APB11, SA1, AA for Indirect Access.
12. Section 5.6.2.2.2 Advanced Authentication Decision Tree: added steps related to the use of compensating controls, Spring 2013, APB12, SA8, compensating controls for AA on smartphones.
13. Figure 8 Advanced Authentication Use Cases: added “Use Case 7 – Advanced Authentication Compensating Controls on Agency Issued Smartphones”, Spring 2013, APB12, SA8, compensating controls for AA on smartphones.
14. Figure 10 Advanced Authentication Decision Tree: updated tree to remove steps related to the Interim Compliance, Spring 2013, APB12, SA5, AA exemption for police vehicles.
15. Figure 10 Advanced Authentication Decision Tree: updated tree to include steps related to the use of compensating controls, Spring 2013, APB12, SA8, compensating controls for AA on smartphones.
16. Section 5.8.2.1 Electronic Media in Transit: changed section title to Digital Media during Transit and modify language, Fall 2013, APB11, SA6, Future CSP for Mobile Devices.
17. Section 5.9.1 Physically Secure Location: added language for police vehicle, Spring 2013, APB12, SA5, AA exemption for police vehicles.
18. Section 5.9.1 Physically Secure Location: removed Interim Compliance language, Spring 2013, APB12, SA5, AA exemption for police vehicles.

19. Section 5.10 System and Communications Protection and Information Integrity: added reference to new Section 5.13.4, Fall 2013, APB11, SA6, Future CSP for Mobile Devices.
20. Section 5.10.1.2 Encryption: added language for passphrase, Fall 2013, APB11, SA3, Encryption standards for CJI at rest.
21. Section 5.10.1.2 Encryption: added language for encryption exception, Fall 2013, APB11, SA3, Encryption standards for CJI at rest.
22. Section 5.10.4.4 Personal Firewall: moved to new Section 5.13.4.5, Fall 2013, APB11, SA6, Future CSP for Mobile Devices.
23. Policy Area 5.13 Mobile Device Security: added new policy area and approved changes to affected policy sections, Fall 2013, APB11, SA6, Future CSP for Mobile Devices.
24. Appendix A Terms and Definitions: added definition for Compensating Controls, Digital Media, Indirect Access, Laptop Devices, Physical Media, Pocket/Handheld Mobile Devices, Receive-Only Terminal (ROT), Smartphone, Tablet Devices, various APB actions.
25. Appendix A Terms and Definitions: added “, a police vehicle,” to definition of Physically Secure Location, Spring 2013, APB12, SA5, AA exemption for police vehicles.
26. Appendix A Terms and Definitions: removed Interim Compliance language from definition of Physically Secure Location, Spring 2013, APB12, SA5, AA exemption for police vehicles.
27. Appendix B Acronyms: added LMR – Land Mobile Radio, Fall 2013, APB11, SA6, Future CSP for Mobile Devices.
28. Appendix G-5 PIN: deleted appendix, Fall 2013, APB11, SA6, Future CSP for Mobile Devices.

Administrative Changes

1. Section 3.2.7 Agency Coordinator #9: changed ‘CJA’ to ‘CGA’
2. Section 4.2.2 NCIC Restricted Files: removed current 4. Immigration Violator File (formerly the Deported Felon Files) and renumber list
3. Section 4.2.2 NCIC Restricted Files: added new file categories; Violent Persons File, NICS Denied Transaction File
4. Section 5.5.2.4 Access Control Mechanisms #3: removed language for consistency based on Fall 2013, APB11, SA3, Encryption standards for CJI at rest
5. Section 5.5.8 References/Citations/Directives: renumbered due to prior section change
6. Section 5.6.2.2.2 Advanced Authentication Decision Tree #2: removed language for consistency based on Spring 2013, APB12, SA5, AA exemption for police vehicles
7. Section 5.6.2.2.2 Advanced Authentication Decision Tree #5: removed language for consistency based on Spring 2013, APB12, SA5, AA exemption for police vehicles
8. Section 5.9.1.1 Security Perimeter: added ‘a’ to first sentence
9. Sections 5.10.4.5 & 5.10.4.6: renumbered due to prior section change
10. Appendix A Terms and Definitions, Agency Coordinator: changed ‘CJA’ to ‘CGA’
11. Appendix D.2 Management Control Agreement: added language to bullet (2)
12. Appendix D.2 Management Control Agreement: added opening quote to reference to Section 5.1.1.4

13. Appendix F.1 IT Security Incident Response Form: added line for affected system descriptor/function (i.e. file server, RMS server, web server, workstation, etc...)
14. Appendix H Security Addendum: changed 'CJA' to 'CGA'
15. Appendix I first reference: added end quote after reference title

KEY TO APB APPROVED CHANGES (i.e. "Fall 2013, APB11, SA6, Future CSP for Mobile Devices"):

Fall 2013 – Advisory Policy Board cycle and year

APB## – Advisory Policy Board Topic number

SA# – Security and Access Subcommittee Topic number

Topic Title

TABLE OF CONTENTS

Executive Summary	i
Change Management.....	ii
Summary of Changes.....	iii
Table of Contents	vi
List of Figures.....	xi
1 Introduction.....	1
1.1 Purpose.....	1
1.2 Scope.....	1
1.3 Relationship to Local Security Policy and Other Policies	1
1.4 Terminology Used in This Document.....	2
1.5 Distribution of the CJIS Security Policy.....	2
2 CJIS Security Policy Approach	3
2.1 CJIS Security Policy Vision Statement.....	3
2.2 Architecture Independent.....	3
2.3 Risk Versus Realism	3
3 Roles and Responsibilities	4
3.1 Shared Management Philosophy.....	4
3.2 Roles and Responsibilities for Agencies and Parties.....	4
3.2.1 CJIS Systems Agencies (CSA)	5
3.2.2 CJIS Systems Officer (CSO).....	5
3.2.3 Terminal Agency Coordinator (TAC).....	6
3.2.4 Criminal Justice Agency (CJA).....	6
3.2.5 Noncriminal Justice Agency (NCJA).....	6
3.2.6 Contracting Government Agency (CGA)	7
3.2.7 Agency Coordinator (AC).....	7
3.2.8 CJIS Systems Agency Information Security Officer (CSA ISO)	7
3.2.9 Local Agency Security Officer (LASO)	8
3.2.10 FBI CJIS Division Information Security Officer (FBI CJIS ISO)	8
3.2.11 Repository Manager	9
3.2.12 Compact Officer.....	9
4 Criminal Justice Information and Personally Identifiable Information	10
4.1 Criminal Justice Information (CJI)	10
4.1.1 Criminal History Record Information (CHRI).....	10
4.2 Access, Use and Dissemination of Criminal History Record Information (CHRI), NCIC Restricted Files Information, and NCIC Non-Restricted Files Information.....	11
4.2.1 Proper Access, Use, and Dissemination of CHRI.....	11
4.2.2 Proper Access, Use, and Dissemination of NCIC Restricted Files Information.....	11
4.2.3 Proper Access, Use, and Dissemination of NCIC Non-Restricted Files Information.....	11
4.2.3.1 For Official Purposes	11
4.2.3.2 For Other Authorized Purposes	12
4.2.3.3 CSO Authority in Other Circumstances	12
4.2.4 Storage.....	12
4.2.5 Justification and Penalties	12
4.2.5.1 Justification	12

4.2.5.2	Penalties	12
4.3	Personally Identifiable Information (PII).....	12
5	Policy and Implementation	14
5.1	Policy Area 1: Information Exchange Agreements	15
5.1.1	Information Exchange	15
5.1.1.1	Information Handling.....	15
5.1.1.2	State and Federal Agency User Agreements	15
5.1.1.3	Criminal Justice Agency User Agreements	16
5.1.1.4	Interagency and Management Control Agreements	16
5.1.1.5	Private Contractor User Agreements and CJIS Security Addendum.....	16
5.1.1.6	Agency User Agreements	17
5.1.1.7	Outsourcing Standards for Channelers	17
5.1.1.8	Outsourcing Standards for Non-Channelers	18
5.1.2	Monitoring, Review, and Delivery of Services.....	18
5.1.2.1	Managing Changes to Service Providers	18
5.1.3	Secondary Dissemination.....	18
5.1.4	Secondary Dissemination of Non-CHRI CJI	18
5.1.5	References/Citations/Directives	19
5.2	Policy Area 2: Security Awareness Training.....	20
5.2.1	Awareness Topics	20
5.2.1.1	All Personnel.....	20
5.2.1.2	Personnel with Physical and Logical Access.....	20
5.2.1.3	Personnel with Information Technology Roles	21
5.2.2	Security Training Records.....	21
5.2.3	References/Citations/Directives	22
5.3	Policy Area 3: Incident Response	23
5.3.1	Reporting Information Security Events.....	23
5.3.1.1	Reporting Structure and Responsibilities.....	23
5.3.1.1.1	FBI CJIS Division Responsibilities	23
5.3.1.1.2	CSA ISO Responsibilities.....	24
5.3.2	Management of Information Security Incidents.....	24
5.3.2.1	Incident Handling.....	24
5.3.2.2	Collection of Evidence.....	24
5.3.3	Incident Response Training.....	24
5.3.4	Incident Monitoring.....	25
5.3.5	References/Citations/Directives	25
5.4	Policy Area 4: Auditing and Accountability.....	26
5.4.1	Auditable Events and Content (Information Systems).....	26
5.4.1.1	Events.....	26
5.4.1.1.1	Content.....	27
5.4.2	Response to Audit Processing Failures	27
5.4.3	Audit Monitoring, Analysis, and Reporting.....	27
5.4.4	Time Stamps.....	27
5.4.5	Protection of Audit Information.....	27
5.4.6	Audit Record Retention.....	28
5.4.7	Logging NCIC and III Transactions.....	28

5.4.8	References/Citations/Directives	28
5.5	Policy Area 5: Access Control.....	29
5.5.1	Account Management	29
5.5.2	Access Enforcement.....	29
5.5.2.1	Least Privilege	30
5.5.2.2	System Access Control	30
5.5.2.3	Access Control Criteria.....	30
5.5.2.4	Access Control Mechanisms.....	30
5.5.3	Unsuccessful Login Attempts	31
5.5.4	System Use Notification.....	31
5.5.5	Session Lock	32
5.5.6	Remote Access	32
5.5.6.1	Personally Owned Information Systems.....	32
5.5.6.2	Publicly Accessible Computers	32
5.5.7	References/Citations/Directives	32
5.6	Policy Area 6: Identification and Authentication	34
5.6.1	Identification Policy and Procedures.....	34
5.6.1.1	Use of Originating Agency Identifiers in Transactions and Information Exchanges	34
5.6.2	Authentication Policy and Procedures	34
5.6.2.1	Standard Authenticators.....	35
5.6.2.1.1	Password	35
5.6.2.1.2	Personal Identification Number (PIN)	35
5.6.2.2	Advanced Authentication.....	36
5.6.2.2.1	Advanced Authentication Policy and Rationale	36
5.6.2.2.2	Advanced Authentication Decision Tree	38
5.6.3	Identifier and Authenticator Management	40
5.6.3.1	Identifier Management.....	40
5.6.3.2	Authenticator Management.....	40
5.6.4	Assertions	40
5.6.5	References/Citations/Directives	41
5.7	Policy Area 7: Configuration Management	47
5.7.1	Access Restrictions for Changes	47
5.7.1.1	Least Functionality.....	47
5.7.1.2	Network Diagram.....	47
5.7.2	Security of Configuration Documentation	47
5.7.3	References/Citations/Directives	47
5.8	Policy Area 8: Media Protection.....	49
5.8.1	Media Storage and Access	49
5.8.2	Media Transport	49
5.8.2.1	Digital Media during Transport	49
5.8.2.2	Physical Media in Transit	49
5.8.3	Electronic Media Sanitization and Disposal	49
5.8.4	Disposal of Physical Media.....	49
5.8.5	References/Citations/Directives	50
5.9	Policy Area 9: Physical Protection	51

5.9.1	Physically Secure Location	51
5.9.1.1	Security Perimeter	51
5.9.1.2	Physical Access Authorizations	51
5.9.1.3	Physical Access Control	51
5.9.1.4	Access Control for Transmission Medium	51
5.9.1.5	Access Control for Display Medium	51
5.9.1.6	Monitoring Physical Access	52
5.9.1.7	Visitor Control	52
5.9.1.8	Delivery and Removal	52
5.9.2	Controlled Area	52
5.9.3	References/Citations/Directives	52
5.10	Policy Area 10: System and Communications Protection and Information Integrity	53
5.10.1	Information Flow Enforcement	53
5.10.1.1	Boundary Protection	53
5.10.1.2	Encryption	54
5.10.1.3	Intrusion Detection Tools and Techniques	55
5.10.1.4	Voice over Internet Protocol	55
5.10.1.5	Cloud Computing	56
5.10.2	Facsimile Transmission of CJI	56
5.10.3	Partitioning and Virtualization	56
5.10.3.1	Partitioning	56
5.10.3.2	Virtualization	56
5.10.4	System and Information Integrity Policy and Procedures	57
5.10.4.1	Patch Management	57
5.10.4.2	Malicious Code Protection	57
5.10.4.3	Spam and Spyware Protection	58
5.10.4.4	Security Alerts and Advisories	58
5.10.4.5	Information Input Restrictions	58
5.10.5	References/Citations/Directives	58
5.11	Policy Area 11: Formal Audits	60
5.11.1	Audits by the FBI CJIS Division	60
5.11.1.1	Triennial Compliance Audits by the FBI CJIS Division	60
5.11.1.2	Triennial Security Audits by the FBI CJIS Division	60
5.11.2	Audits by the CSA	60
5.11.3	Special Security Inquiries and Audits	60
5.11.4	References/Citations/Directives	60
5.12	Policy Area 12: Personnel Security	62
5.12.1	Personnel Security Policy and Procedures	62
5.12.1.1	Minimum Screening Requirements for Individuals Requiring Access to CJI	62
5.12.1.2	Personnel Screening for Contractors and Vendors	63
5.12.2	Personnel Termination	63
5.12.3	Personnel Transfer	64
5.12.4	Personnel Sanctions	64
5.12.5	References/Citations/Directives	64
5.13	Policy Area 13: Mobile Devices	65
5.13.1	Wireless Communications Technologies	65

5.13.1.1 All 802.11 Wireless Protocols	65
5.13.1.2 Cellular.....	66
5.13.1.2.1 Cellular Service Abroad.....	66
5.13.1.2.2 Voice Transmissions Over Cellular Devices	67
5.13.1.3 Bluetooth.....	67
5.13.2 Mobile Device Management (MDM)	67
5.13.3 Wireless Device Risk Mitigations.....	68
5.13.3.1 Legacy 802.11 Protocols.....	68
5.13.4 System Integrity	68
5.13.4.1 Patching/Updates	68
5.13.4.2 Malicious Code Protection.....	69
5.13.4.3 Physical Protection.....	69
5.13.4.4 Personal Firewall	69
5.13.5 Incident Response	70
5.13.6 Auditing and Accountability	70
5.13.7 Access Control	70
5.13.8 Wireless Hotspot Capability.....	71
5.13.9 Identification and Authentication.....	71
5.13.9.1 Local Device Authentication	71
5.13.10 Device Certificates	71
Appendices.....	A-1
Appendix A Terms and Definitions	A-1
Appendix B Acronyms	B-1
Appendix C Network Topology Diagrams	C-1
Appendix D Sample Information Exchange Agreements.....	D-1
D.1 CJIS User Agreement	D-1
D.2 Management Control Agreement.....	D-9
D.3 Noncriminal Justice Agency Agreement & Memorandum of Understanding.....	D-10
D.4 Interagency Connection Agreement	D-16
Appendix E Security Forums and Organizational Entities.....	E-1
Appendix F Sample Forms.....	F-1
F.1 IT Security Incident Response Form	F-2
Appendix G Best practices	G-1
G.1 Virtualization	G-1
G.2 Voice over Internet Protocol White Paper	G-4
G.3 Cloud Computing White Paper	G-15
G.4 Mobile Appendix	G-30
Appendix H Security Addendum	H-1
Appendix I References	I-1
Appendix J Noncriminal Justice Agency Supplemental Guidance	J-1
Appendix K Criminal Justice Agency Supplemental Guidance	K-1

LIST OF FIGURES

Figure 1 – Overview Diagram of Strategic Functions and Policy Components	4
Figure 2 – Dissemination of restricted and non-restricted NCIC data.....	13
Figure 3 – Information Exchange Agreements Implemented by a Local Police Department	19
Figure 4 – Security Awareness Training Implemented by a Local Police Department.....	22
Figure 5 – Incident Response Process Initiated by an Incident in a Local Police Department	25
Figure 6 – Local Police Department's Use of Audit Logs	28
Figure 7 – A Local Police Department's Access Controls	33
Figure 8 – Advanced Authentication Use Cases.....	41
Figure 9 – Authentication Decision for Known Location	45
Figure 10 – Authentication Decision for Unknown Location	46
Figure 11 – A Local Police Department's Configuration Management Controls	48
Figure 12 – A Local Police Department's Media Management Policies.....	50
Figure 13 – A Local Police Department's Physical Protection Measures.....	52
Figure 14 – A Local Police Department's Information Systems & Communications Protections	59
Figure 15 – The Audit of a Local Police Department.....	61
Figure 16 – A Local Police Department's Personnel Security Controls	64

1 INTRODUCTION

This section details the purpose of this document, its scope, relationship to other information security policies, and its distribution constraints.

1.1 Purpose

The CJIS Security Policy provides Criminal Justice Agencies (CJA) and Noncriminal Justice Agencies (NCJA) with a minimum set of security requirements for access to Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division systems and information and to protect and safeguard Criminal Justice Information (CJI). This minimum standard of security requirements ensures continuity of information protection. The essential premise of the CJIS Security Policy is to provide the appropriate controls to protect CJI, from creation through dissemination; whether at rest or in transit.

The CJIS Security Policy integrates presidential directives, federal laws, FBI directives, the criminal justice community's Advisory Policy Board (APB) decisions along with nationally recognized guidance from the National Institute of Standards and Technology (NIST) and the National Crime Prevention and Privacy Compact Council (Compact Council).

1.2 Scope

At the consent of the advisory process, and taking into consideration federal law and state statutes, the CJIS Security Policy applies to all entities with access to, or who operate in support of, FBI CJIS Division's services and information. The CJIS Security Policy provides minimum security requirements associated with the creation, viewing, modification, transmission, dissemination, storage, or destruction of CJI.

Entities engaged in the interstate exchange of CJI data for noncriminal justice purposes are also governed by the standards and rules promulgated by the Compact Council.

1.3 Relationship to Local Security Policy and Other Policies

The CJIS Security Policy may be used as the sole security policy for the agency. The local agency may complement the CJIS Security Policy with a local policy, or the agency may develop their own stand-alone security policy; however, the CJIS Security Policy shall always be the minimum standard and local policy may augment, or increase the standards, but shall not detract from the CJIS Security Policy standards.

The agency shall develop, disseminate, and maintain formal, documented procedures to facilitate the implementation of the CJIS Security Policy and, where applicable, the local security policy. The policies and procedures shall be consistent with applicable laws, executive orders, directives, policies, regulations, standards, and guidance. Procedures developed for CJIS Security Policy areas can be developed for the security program in general, and for a particular information system, when required.

This document is a compendium of applicable policies in providing guidance on the minimum security controls and requirements needed to access FBI CJIS information and services. These policies include presidential directives, federal laws, FBI directives and the criminal justice community's APB decisions. State, local, and Tribal CJA may implement more stringent

policies and requirements. Appendix I contains the references while Appendix E lists the security forums and organizational entities referenced in this document.

1.4 Terminology Used in This Document

The following terms are used interchangeably throughout this document:

- Agency and Organization: The two terms in this document refer to any entity that submits or receives information, by any means, to/from FBI CJIS systems or services.
- Information and Data: Both terms refer to CJI.
- System, Information System, Service, or named applications like NCIC: all refer to connections to the FBI's criminal justice information repositories and the equipment used to establish said connections.

Appendix A and B provide an extensive list of the terms and acronyms.

1.5 Distribution of the CJIS Security Policy

The CJIS Security Policy, version 5.0 and later, is a publically available document and may be posted and shared without restrictions.

2 CJIS SECURITY POLICY APPROACH

The CJIS Security Policy represents the shared responsibility between FBI CJIS, CJIS Systems Agency (CSA), and the State Identification Bureaus (SIB) of the lawful use and appropriate protection of CJL. The Policy provides a baseline of security requirements for current and planned services and sets a minimum standard for new initiatives.

2.1 CJIS Security Policy Vision Statement

The executive summary of this document describes the vision in terms of business needs for confidentiality, integrity, and availability of information. The APB collaborates with the FBI CJIS Division to ensure that the Policy remains updated to meet evolving business, technology and security needs.

2.2 Architecture Independent

Due to advancing technology and evolving business models, the FBI CJIS Division is transitioning from legacy stovepipe systems and moving toward a flexible services approach. Systems such as National Crime Information Center (NCIC), National Instant Criminal Background Check System (NICS), and Integrated Automated Fingerprint Identification System (IAFIS) will continue to evolve and may no longer retain their current system platforms, hardware, or program name. However, the data and services provided by these systems will remain stable.

The CJIS Security Policy looks at the data (information), services, and protection controls that apply regardless of the implementation architecture. Architectural independence is not intended to lessen the importance of systems, but provide for the replacement of one technology with another while ensuring the controls required to protect the information remain constant. This objective and conceptual focus on security policy areas provide the guidance and standards while avoiding the impact of the constantly changing landscape of technical innovations. The architectural independence of the Policy provides agencies with the flexibility for tuning their information security infrastructure and policies to reflect their own environments.

2.3 Risk Versus Realism

Every “shall” statement contained within the CJIS Security Policy has been scrutinized for risk versus the reality of resource constraints and real-world application. The purpose of the CJIS Security Policy is to establish the minimum security requirements; therefore, individual agencies are encouraged to implement additional controls to address agency specific risks.

3 ROLES AND RESPONSIBILITIES

3.1 Shared Management Philosophy

In the scope of information security, the FBI CJIS Division employs a shared management philosophy with federal, state, local, and tribal law enforcement agencies. Although an advisory policy board for the NCIC has existed since 1969, the Director of the FBI established the CJIS APB in March 1994 to enable appropriate input and recommend policy with respect to CJIS services. Through the APB and its Subcommittees and Working Groups, consideration is given to the needs of the criminal justice and law enforcement community regarding public policy, statutory and privacy aspects, as well as national security relative to CJIS systems and information. The APB represents federal, state, local, and tribal law enforcement and criminal justice agencies throughout the United States, its territories, and Canada.

The FBI has a similar relationship with the Compact Council, which governs the interstate exchange of criminal history records for noncriminal justice purposes. The Compact Council is mandated by federal law to promulgate rules and procedures for the use of the Interstate Identification Index (III) for noncriminal justice purposes. To meet that responsibility, the Compact Council depends on the CJIS Security Policy as the definitive source for standards defining the security and privacy of records exchanged with noncriminal justice practitioners.

3.2 Roles and Responsibilities for Agencies and Parties

It is the responsibility of all agencies covered under this Policy to ensure the protection of CJI between the FBI CJIS Division and its user community. The following figure provides an abstract representation of the strategic functions and roles such as governance and operations.

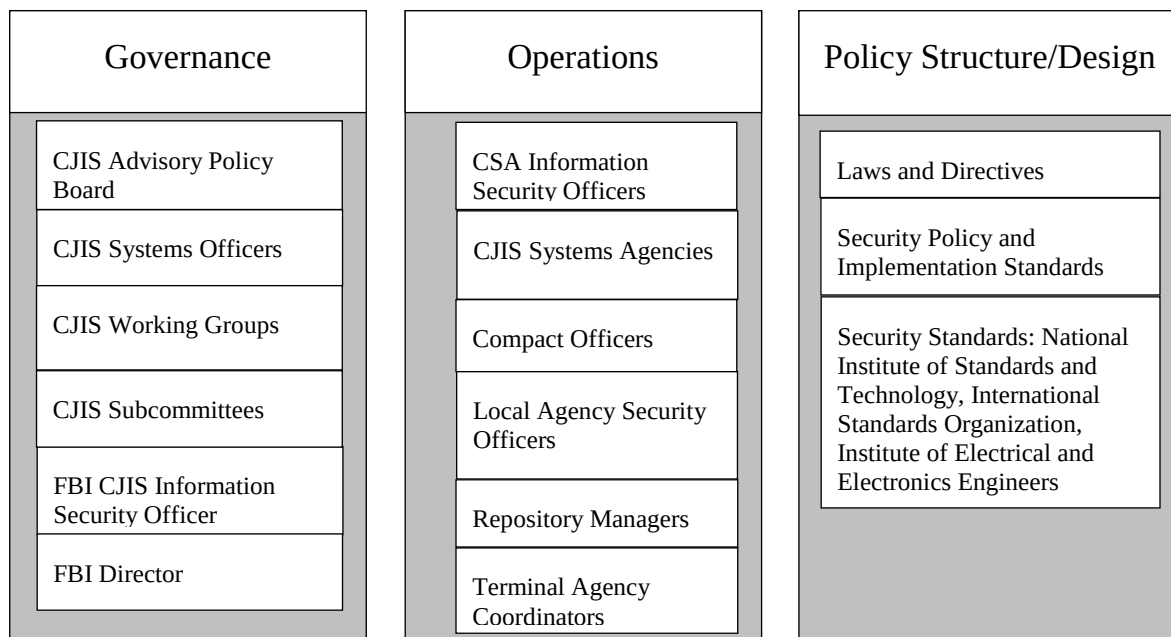


Figure 1 – Overview Diagram of Strategic Functions and Policy Components

This section provides a description of the following entities and roles:

1. CJIS Systems Agency.
2. CJIS Systems Officer.
3. Terminal Agency Coordinator.
4. Criminal Justice Agency.
5. Noncriminal Justice Agency.
6. Contracting Government Agency.
7. Agency Coordinator.
8. CJIS Systems Agency Information Security Officer.
9. Local Agency Security Officer.
10. FBI CJIS Division Information Security Officer.
11. Repository Manager.
12. Compact Officer.

3.2.1 CJIS Systems Agencies (CSA)

The CSA is responsible for establishing and administering an information technology security program throughout the CSA's user community, to include the local levels. The head of each CSA shall appoint a CJIS Systems Officer (CSO). The CSA may impose more stringent protection measures than outlined in this document. Such decisions shall be documented and kept current.

3.2.2 CJIS Systems Officer (CSO)

The CSO is an individual located within the CSA responsible for the administration of the CJIS network for the CSA. Pursuant to the Bylaws for the CJIS Advisory Policy Board and Working Groups, the role of CSO shall not be outsourced. The CSO may delegate responsibilities to subordinate agencies. The CSO shall set, maintain, and enforce the following:

1. Standards for the selection, supervision, and separation of personnel who have access to CJI.
2. Policy governing the operation of computers, access devices, circuits, hubs, routers, firewalls, and other components that comprise and support a telecommunications network and related CJIS systems used to process, store, or transmit CJI, guaranteeing the priority, confidentiality, integrity, and availability of service needed by the criminal justice community.
 - a. Ensure appropriate use, enforce system discipline, and ensure CJIS Division operating procedures are followed by all users of the respective services and information.
 - b. Ensure state/federal agency compliance with policies approved by the APB and adopted by the FBI.

- c. Ensure the appointment of the CSA ISO and determine the extent of authority to the CSA ISO.
- d. The CSO, or designee, shall ensure that a Terminal Agency Coordinator (TAC) is designated within each agency that has devices accessing CJIS systems.
- e. Ensure each agency having access to CJI has someone designated as the Local Agency Security Officer (LASO).
- f. Approve access to FBI CJIS systems.
- g. Assume ultimate responsibility for managing the security of CJIS systems within their state and/or agency.
- h. Perform other related duties outlined by the user agreements with the FBI CJIS Division.

3. Outsourcing of Criminal Justice Functions

- a. Responsibility for the management of the approved security requirements shall remain with the CJA. Security control includes the authority to enforce the standards for the selection, supervision, and separation of personnel who have access to CJI; set and enforce policy governing the operation of computers, circuits, and telecommunications terminals used to process, store, or transmit CJI; and to guarantee the priority service needed by the criminal justice community.
- b. Responsibility for the management control of network security shall remain with the CJA. Management control of network security includes the authority to enforce the standards for the selection, supervision, and separation of personnel who have access to CJI; set and enforce policy governing the operation of circuits and network equipment used to transmit CJI; and to guarantee the priority service as determined by the criminal justice community.

3.2.3 Terminal Agency Coordinator (TAC)

The TAC serves as the point-of-contact at the local agency for matters relating to CJIS information access. The TAC administers CJIS systems programs within the local agency and oversees the agency's compliance with CJIS systems policies.

3.2.4 Criminal Justice Agency (CJA)

A CJA is defined as a court, a governmental agency, or any subunit of a governmental agency which performs the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice. State and federal Inspectors General Offices are included.

3.2.5 Noncriminal Justice Agency (NCJA)

A NCJA is defined (for the purposes of access to CJI) as an entity or any subunit thereof that provides services primarily for purposes other than the administration of criminal justice.

3.2.6 Contracting Government Agency (CGA)

A CGA is a government agency, whether a CJA or a NCJA, that enters into an agreement with a private contractor subject to the CJIS Security Addendum. The CGA entering into an agreement with a contractor shall appoint an agency coordinator.

3.2.7 Agency Coordinator (AC)

An AC is a staff member of the CGA who manages the agreement between the Contractor and agency. The AC shall be responsible for the supervision and integrity of the system, training and continuing education of employees and operators, scheduling of initial training and testing, and certification testing and all required reports by NCIC. The AC shall:

1. Understand the communications, records capabilities, and needs of the Contractor which is accessing federal and state records through or because of its relationship with the CGA.
2. Participate in related meetings and provide input and comments for system improvement.
3. Receive information from the CGA (e.g., system updates) and disseminate it to appropriate Contractor employees.
4. Maintain and update manuals applicable to the effectuation of the agreement, and provide them to the Contractor.
5. Maintain up-to-date records of Contractor's employees who access the system, including name, date of birth, social security number, date fingerprint card(s) submitted, date security clearance issued, and date initially trained, tested, certified or recertified (if applicable).
6. Train or ensure the training of Contractor personnel. If Contractor personnel access NCIC, schedule the operators for testing or a certification exam with the CSA staff, or AC staff with permission from the CSA staff. Schedule new operators for the certification exam within six (6) months of assignment. Schedule certified operators for biennial re-certification testing within thirty (30) days prior to the expiration of certification. Schedule operators for other mandated class.
7. The AC will not permit an untrained/untested or non-certified Contractor employee to access CJI or systems supporting CJI where access to CJI can be gained.
8. Where appropriate, ensure compliance by the Contractor with NCIC validation requirements.
9. Provide completed applicant fingerprint cards on each Contractor employee who accesses the system to the CGA (or, where appropriate, CSA) for criminal background investigation prior to such employee accessing the system.
10. Any other responsibility for the AC promulgated by the FBI.

3.2.8 CJIS Systems Agency Information Security Officer (CSA ISO)

The CSA ISO shall:

1. Serve as the security point of contact (POC) to the FBI CJIS Division ISO.

2. Document technical compliance with the CJIS Security Policy with the goal to assure the confidentiality, integrity, and availability of criminal justice information to the user community throughout the CSA's user community, to include the local level.
3. Document and provide assistance for implementing the security-related controls for the Interface Agency and its users.
4. Establish a security incident response and reporting procedure to discover, investigate, document, and report to the CSA, the affected criminal justice agency, and the FBI CJIS Division ISO major incidents that significantly endanger the security or integrity of CJI.

3.2.9 Local Agency Security Officer (LASO)

Each LASO shall:

1. Identify who is using the CSA approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.
2. Identify and document how the equipment is connected to the state system.
3. Ensure that personnel security screening procedures are being followed as stated in this Policy.
4. Ensure the approved and appropriate security measures are in place and working as expected.
5. Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.

3.2.10 FBI CJIS Division Information Security Officer (FBI CJIS ISO)

The FBI CJIS ISO shall:

1. Maintain the CJIS Security Policy.
2. Disseminate the FBI Director approved CJIS Security Policy.
3. Serve as a liaison with the CSA's ISO and with other personnel across the CJIS community and in this regard provide technical guidance as to the intent and implementation of operational and technical policy issues.
4. Serve as a point-of-contact (POC) for computer incident notification and distribution of security alerts to the CSOs and ISOs.
5. Assist with developing audit compliance guidelines as well as identifying and reconciling security-related issues.
6. Develop and participate in information security training programs for the CSOs and ISOs, and provide a means by which to acquire feedback to measure the effectiveness and success of such training.
7. Maintain a security policy resource center (SPRC) on FBI.gov and keep the CSOs and ISOs updated on pertinent information.

3.2.11 Repository Manager

The State Identification Bureau (SIB) Chief, i.e. Repository Manager or Chief Administrator, is the designated manager of the agency having oversight responsibility for a state's fingerprint identification services. If both state fingerprint identification services and CJIS systems control are managed within the same state agency, the SIB Chief and CSO may be the same person.

3.2.12 Compact Officer

Pursuant to the National Crime Prevention and Privacy Compact, each party state shall appoint a Compact Officer who shall ensure that Compact provisions and rules, procedures, and standards established by the Compact Council are complied with in their respective state.

4 CRIMINAL JUSTICE INFORMATION AND PERSONALLY IDENTIFIABLE INFORMATION

4.1 Criminal Justice Information (CJI)

Criminal Justice Information is the term used to refer to all of the FBI CJIS provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data. The following categories of CJI describe the various data sets housed by the FBI CJIS architecture:

1. **Biometric Data**—data derived from one or more intrinsic physical or behavioral traits of humans typically for the purpose of uniquely identifying individuals from within a population. Used to identify individuals, to include: fingerprints, palm prints, iris scans, and facial recognition data.
2. **Identity History Data**—textual data that corresponds with an individual’s biometric data, providing a history of criminal and/or civil events for the identified individual.
3. **Biographic Data**—information about individuals associated with a unique case, and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case.
4. **Property Data**—information about vehicles and property associated with crime when accompanied by any personally identifiable information (PII).
5. **Case/Incident History**—information about the history of criminal incidents.

The following type of data are exempt from the protection levels required for CJI: transaction control type numbers (e.g., ORI, NIC, FNU, etc.) when not accompanied by information that reveals CJI or PII.

The intent of the CJIS Security Policy is to ensure the protection of the aforementioned CJI until the information is: released to the public via authorized dissemination (e.g. within a court system; presented in crime reports data; released in the interest of public safety); purged or destroyed in accordance with applicable record retention rules.

4.1.1 Criminal History Record Information (CHRI)

Criminal History Record Information (CHRI), sometimes informally referred to as “restricted data”, is a subset of CJI. Due to its comparatively sensitive nature, additional controls are required for the access, use and dissemination of CHRI. In addition to the dissemination restrictions outlined below, Title 28, Part 20, Code of Federal Regulations (CFR), defines CHRI and provides the regulatory guidance for dissemination of CHRI. While the CJIS Security Policy attempts to be architecturally independent, the III and the NCIC are specifically identified in Title 28, Part 20, CFR, and the NCIC Operating Manual, as associated with CHRI.

4.2 Access, Use and Dissemination of Criminal History Record Information (CHRI), NCIC Restricted Files Information, and NCIC Non-Restricted Files Information

This section describes the requirements for the access, use and dissemination of CHRI, NCIC restricted files information, and NCIC non-restricted files information.

4.2.1 Proper Access, Use, and Dissemination of CHRI

Information obtained from the III is considered CHRI. Rules governing the access, use, and dissemination of CHRI are found in Title 28, Part 20, CFR. The III shall be accessed only for an authorized purpose. Further, CHRI shall only be used for an authorized purpose consistent with the purpose for which III was accessed. Dissemination to another agency is authorized if (a) the other agency is an Authorized Recipient of such information and is being serviced by the accessing agency, or (b) the other agency is performing personnel and appointment functions for criminal justice employment applicants.

4.2.2 Proper Access, Use, and Dissemination of NCIC Restricted Files Information

The NCIC hosts restricted files and non-restricted files. NCIC restricted files are distinguished from NCIC non-restricted files by the policies governing their access and use. Proper access to, use, and dissemination of data from restricted files shall be consistent with the access, use, and dissemination policies concerning the III described in Title 28, Part 20, CFR, and the NCIC Operating Manual. The restricted files, which shall be protected as CHRI, are as follows:

1. Gang Files
2. Known or Appropriately Suspected Terrorist Files
3. Supervised Release Files
4. National Sex Offender Registry Files
5. Historical Protection Order Files of the NCIC
6. Identity Theft Files
7. Protective Interest Files
8. Person With Information (PWI) data in the Missing Person Files
9. Violent Person File
10. NICS Denied Transactions File

The remaining NCIC files are considered non-restricted files.

4.2.3 Proper Access, Use, and Dissemination of NCIC Non-Restricted Files Information

4.2.3.1 For Official Purposes

NCIC non-restricted files are those not listed as restricted files in Section 4.2.2. NCIC non-restricted files information may be accessed and used for any authorized purpose consistent with

the inquiring agency's responsibility. Information obtained may be disseminated to (a) other government agencies or (b) private entities authorized by law to receive such information for any purpose consistent with their responsibilities.

4.2.3.2 For Other Authorized Purposes

NCIC non-restricted files may be accessed for other purposes consistent with the resources of the inquiring agency; however, requests for bulk data are discouraged. Information derived from NCIC non-restricted files for other than law enforcement purposes can be used by authorized criminal justice personnel only to confirm the status of a person or property (i.e., wanted or stolen). An inquiring agency is authorized to charge a nominal administrative fee for such service. Non-restricted files information shall not be disseminated commercially.

A response to a NCIC person inquiry may include NCIC restricted files information as well as NCIC non-restricted files information. Agencies shall not disseminate restricted files information for purposes other than law enforcement.

4.2.3.3 CSO Authority in Other Circumstances

If no federal, state or local law or policy prohibition exists, the CSO may exercise discretion to approve or deny dissemination of NCIC non-restricted file information.

4.2.4 Storage

When CHRI is stored, agencies shall establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of the information. These records shall be stored for extended periods only when they are key elements for the integrity and/or utility of case files and/or criminal record files. See Section 5.9 for physical security controls.

4.2.5 Justification and Penalties

4.2.5.1 Justification

In addition to the use of purpose codes and logging information, all users shall provide a reason for all III inquiries whenever requested by NCIC System Managers, CSAs, local agency administrators, or their representatives.

4.2.5.2 Penalties

Improper access, use or dissemination of CHRI and NCIC Non-Restricted Files information is serious and may result in administrative sanctions including, but not limited to, termination of services and state and federal criminal penalties.

4.3 Personally Identifiable Information (PII)

For the purposes of this document, PII is information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. Any FBI CJIS provided data maintained by an agency, including but not limited to, education, financial transactions, medical history, and criminal or employment history may include PII. A criminal history record

for example inherently contains PII as would a Law Enforcement National Data Exchange (N-DEx) case file.

PII shall be extracted from CJI for the purpose of official business only. Agencies shall develop policies, based on state and local privacy rules, to ensure appropriate controls are applied when handling PII extracted from CJI. Due to the expansive nature of PII, this Policy does not specify auditing, logging, or personnel security requirements associated with the life cycle of PII.

Figure 2 – Dissemination of restricted and non-restricted NCIC data

A citizen of Springfield went to the Springfield Police Department to request whether his new neighbor, who had been acting suspiciously, had an outstanding warrant. The Springfield Police Department ran an NCIC persons inquiry, which produced a response that included a Wanted Person File (non-restricted file) record and a Known or Appropriately Suspected Terrorist File (restricted file) record. The Springfield Police Department advised the citizen of the outstanding warrant, but did not disclose any information concerning the subject being a known or appropriately suspected terrorist.

5 POLICY AND IMPLEMENTATION

The policy areas focus upon the data and services that the FBI CJIS Division exchanges and provides to the criminal justice community and its partners. Each policy area provides both strategic reasoning and tactical implementation requirements and standards.

While the major theme of the policy areas is concerned with electronic exchange directly with the FBI, it is understood that further dissemination of CJI to Authorized Recipients by various means (hard copy, e-mail, web posting, etc.) constitutes a significant portion of CJI exchanges. Regardless of its form, use, or method of dissemination, CJI requires protection throughout its life.

Not every consumer of FBI CJIS services will encounter all of the policy areas therefore the circumstances of applicability are based on individual agency/entity configurations and usage. Use cases within each of the policy areas will help users relate the Policy to their own agency circumstances. The policy areas are:

- Policy Area 1—Information Exchange Agreements
- Policy Area 2—Security Awareness Training
- Policy Area 3—Incident Response
- Policy Area 4—Auditing and Accountability
- Policy Area 5—Access Control
- Policy Area 6—Identification and Authentication
- Policy Area 7—Configuration Management
- Policy Area 8—Media Protection
- Policy Area 9—Physical Protection
- Policy Area 10—Systems and Communications Protection and Information Integrity
- Policy Area 11—Formal Audits
- Policy Area 12—Personnel Security

5.1 Policy Area 1: Information Exchange Agreements

The information shared through communication mediums shall be protected with appropriate security safeguards. The agreements established by entities sharing information across systems and communications mediums are vital to ensuring all parties fully understand and agree to a set of security standards.

5.1.1 Information Exchange

Before exchanging CJI, agencies shall put formal agreements in place that specify security controls. The exchange of information may take several forms including electronic mail, instant messages, web services, facsimile, hard copy, and information systems sending, receiving and storing CJI.

Information exchange agreements outline the roles, responsibilities, and data ownership between agencies and any external parties. Information exchange agreements for agencies sharing CJI data that is sent to and/or received from the FBI CJIS shall specify the security controls and conditions described in this document.

Information exchange agreements shall be supported by documentation committing both parties to the terms of information exchange. As described in subsequent sections, different agreements and policies apply, depending on whether the parties involved are CJAs or NCJAs. See Appendix D for examples of Information Exchange Agreements.

There may be instances, on an ad-hoc basis, where CJI is authorized for further dissemination to Authorized Recipients not covered by an information exchange agreement with the releasing agency. In these instances the dissemination of CJI is considered to be secondary dissemination. Law Enforcement and civil agencies shall have a local policy to validate a requestor of CJI as an authorized recipient before disseminating CJI. See Section 5.1.3 for secondary dissemination guidance.

5.1.1.1 Information Handling

Procedures for handling and storage of information shall be established to protect that information from unauthorized disclosure, alteration or misuse. Using the requirements in this Policy as a starting point, the procedures shall apply to the handling, processing, storing, and communication of CJI. These procedures apply to the exchange of CJI no matter the form of exchange.

The policies for information handling and protection also apply to using CJI shared with or received from FBI CJIS for noncriminal justice purposes. In general, a noncriminal justice purpose includes the use of criminal history records for purposes authorized by federal or state law other than purposes relating to the administration of criminal justice, including – but not limited to - employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

5.1.1.2 State and Federal Agency User Agreements

Each CSA head or SIB Chief shall execute a signed written user agreement with the FBI CJIS Division stating their willingness to demonstrate conformity with this Policy before accessing and participating in CJIS records information programs. This agreement shall include the

standards and sanctions governing utilization of CJIS systems. As coordinated through the particular CSA or SIB Chief, each Interface Agency shall also allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system per authorization of Department of Justice (DOJ) Order 2640.2F. All user agreements with the FBI CJIS Division shall be coordinated with the CSA head.

5.1.1.3 Criminal Justice Agency User Agreements

Any CJA receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA providing the access. The written agreement shall specify the FBI CJIS systems and services to which the agency will have access, and the FBI CJIS Division policies to which the agency must adhere. These agreements shall include:

1. Audit.
2. Dissemination.
3. Hit confirmation.
4. Logging.
5. Quality Assurance (QA).
6. Screening (Pre-Employment).
7. Security.
8. Timeliness.
9. Training.
10. Use of the system.
11. Validation.

5.1.1.4 Interagency and Management Control Agreements

A NCJA (government) designated to perform criminal justice functions for a CJA shall be eligible for access to the CJI. Access shall be permitted when such designation is authorized pursuant to executive order, statute, regulation, or inter-agency agreement. The NCJA shall sign and execute a management control agreement (MCA) with the CJA, which stipulates management control of the criminal justice function remains solely with the CJA. The MCA may be a separate document or included with the language of an inter-agency agreement. An example of an NCJA (government) is a city information technology (IT) department.

5.1.1.5 Private Contractor User Agreements and CJIS Security Addendum

The CJIS Security Addendum is a uniform addendum to an agreement between the government agency and a private contractor, approved by the Attorney General of the United States, which specifically authorizes access to CHRI, limits the use of the information to the purposes for which it is provided, ensures the security and confidentiality of the information is consistent with existing regulations and the CJIS Security Policy, provides for sanctions, and contains such other provisions as the Attorney General may require.

Private contractors who perform criminal justice functions shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall

be subject to the same extent of audit review as are local user agencies. All private contractors who perform criminal justice functions shall acknowledge, via signing of the CJIS Security Addendum Certification page, and abide by all aspects of the CJIS Security Addendum. The CJIS Security Addendum is presented in Appendix H. Modifications to the CJIS Security Addendum shall be enacted only by the FBI.

1. Private contractors designated to perform criminal justice functions for a CJA shall be eligible for access to CJI. Access shall be permitted pursuant to an agreement which specifically identifies the agency's purpose and scope of providing services for the administration of criminal justice. The agreement between the CJA and the private contractor shall incorporate the CJIS Security Addendum approved by the Director of the FBI, acting for the U.S. Attorney General, as referenced in Title 28 CFR 20.33 (a)(7).
2. Private contractors designated to perform criminal justice functions on behalf of a NCJA (government) shall be eligible for access to CJI. Access shall be permitted pursuant to an agreement which specifically identifies the agency's purpose and scope of providing services for the administration of criminal justice. The agreement between the NCJA and the private contractor shall incorporate the CJIS Security Addendum approved by the Director of the FBI, acting for the U.S. Attorney General, as referenced in Title 28 CFR 20.33 (a)(7).

5.1.1.6 Agency User Agreements

A NCJA (public) designated to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions, shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. A NCJA (public) receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA/SIB providing the access. An example of a NCJA (public) is a county school board.

A NCJA (private) designated to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions, shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. A NCJA (private) receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA, SIB, or authorized agency providing the access. An example of a NCJA (private) is a local bank.

All NCJAs accessing CJI shall be subject to all pertinent areas of the CJIS Security Policy (see Appendix J for supplemental guidance). Each NCJA that directly accesses FBI CJI shall also allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system per authorization of Department of Justice (DOJ) Order 2640.2F.

5.1.1.7 Outsourcing Standards for Channelers

Channelers designated to request civil fingerprint-based background checks or noncriminal justice ancillary functions on behalf of a NCJA (public) or NCJA (private) for noncriminal justice functions shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney

General. All Channelers accessing CJI shall be subject to the terms and conditions described in the Compact Council Security and Management Control Outsourcing Standard. Each Channeler that directly accesses CJI shall also allow the FBI to conduct periodic penetration testing.

Channelers leveraging CJI to perform civil functions on behalf of an Authorized Recipient shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies.

5.1.1.8 Outsourcing Standards for Non-Channelers

Contractors designated to perform noncriminal justice ancillary functions on behalf of a NCJA (public) or NCJA (private) for noncriminal justice functions shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. All contractors accessing CJI shall be subject to the terms and conditions described in the Compact Council Outsourcing Standard for Non-Channelers. Contractors leveraging CJI to perform civil functions on behalf of an Authorized Recipient shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies.

5.1.2 Monitoring, Review, and Delivery of Services

As specified in the inter-agency agreements, MCAs, and contractual agreements with private contractors, the services, reports and records provided by the service provider shall be regularly monitored and reviewed. The CJA, authorized agency, or FBI shall maintain sufficient overall control and visibility into all security aspects to include, but not limited to, identification of vulnerabilities and information security incident reporting/response. The incident reporting/response process used by the service provider shall conform to the incident reporting/response specifications provided in this Policy.

5.1.2.1 Managing Changes to Service Providers

Any changes to services provided by a service provider shall be managed by the CJA, authorized agency, or FBI. This includes provision of services, changes to existing services, and new services. Evaluation of the risks to the agency shall be undertaken based on the criticality of the data, system, and the impact of the change.

5.1.3 Secondary Dissemination

If CHRI is released to another authorized agency, and that agency was not part of the releasing agency's primary information exchange agreement(s), the releasing agency shall log such dissemination.

5.1.4 Secondary Dissemination of Non-CHRI CJI

If CJI does not contain CHRI and is not part of an information exchange agreement then it does not need to be logged. Dissemination shall conform to the local policy validating the requestor of the CJI as an employee and/or contractor of a law enforcement agency or civil agency requiring the CJI to perform their mission or a member of the public receiving CJI via authorized dissemination.

5.1.5 References/Citations/Directives

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

Figure 3 – Information Exchange Agreements Implemented by a Local Police Department

A local police department executed a Memorandum of Understanding (MOU) for the interface with their state CSA. The local police department also executed an MOU (which included an MCA) with the county information technology (IT) department for the day-to-day operations of their criminal-justice infrastructure. The county IT department, in turn, outsourced operations to a local vendor who signed the CJIS Security Addendum.

5.2 Policy Area 2: Security Awareness Training

Basic security awareness training shall be required within six months of initial assignment, and biennially thereafter, for all personnel who have access to CJI. The CSO/SIB may accept the documentation of the completion of security awareness training from another agency. Accepting such documentation from another agency means that the accepting agency assumes the risk that the training may not meet a particular requirement or process required by federal, state, or local laws.

5.2.1 Awareness Topics

A significant number of topics can be mentioned and briefly discussed in any awareness session or campaign. To help further the development and implementation of individual agency security awareness training programs the following baseline guidance is provided.

5.2.1.1 All Personnel

At a minimum, the following topics shall be addressed as baseline security awareness training for all authorized personnel with access to CJI:

1. Rules that describe responsibilities and expected behavior with regard to CJI usage.
2. Implications of noncompliance.
3. Incident response (Points of contact; Individual actions).
4. Media protection.
5. Visitor control and physical access to spaces—discuss applicable physical security policy and procedures, e.g., challenge strangers, report unusual activity.
6. Protect information subject to confidentiality concerns — hardcopy through destruction.
7. Proper handling and marking of CJI.
8. Threats, vulnerabilities, and risks associated with handling of CJI.
9. Social engineering.
10. Dissemination and destruction.

5.2.1.2 Personnel with Physical and Logical Access

In addition to 5.2.1.1 above, the following topics, at a minimum, shall be addressed as baseline security awareness training for all authorized personnel with both physical and logical access to CJI:

1. Rules that describe responsibilities and expected behavior with regard to information system usage.
2. Password usage and management—including creation, frequency of changes, and protection.
3. Protection from viruses, worms, Trojan horses, and other malicious code.
4. Unknown e-mail/attachments.

5. Web usage—allowed versus prohibited; monitoring of user activity.
6. Spam.
7. Physical Security—increases in risks to systems and data.
8. Handheld device security issues—address both physical and wireless security issues.
9. Use of encryption and the transmission of sensitive/confidential information over the Internet—address agency policy, procedures, and technical contact for assistance.
10. Laptop security—address both physical and information security issues.
11. Personally owned equipment and software—state whether allowed or not (e.g., copyrights).
12. Access control issues—address least privilege and separation of duties.
13. Individual accountability—explain what this means in the agency.
14. Use of acknowledgement statements—passwords, access to systems and data, personal use and gain.
15. Desktop security—discuss use of screensavers, restricting visitors’ view of information on screen (mitigating “shoulder surfing”), battery backup devices, allowed access to systems.
16. Protect information subject to confidentiality concerns—in systems, archived, on backup media, and until destroyed.
17. Threats, vulnerabilities, and risks associated with accessing CJIS Service systems and services.

5.2.1.3 Personnel with Information Technology Roles

In addition to 5.2.1.1 and 5.2.1.2 above, the following topics at a minimum shall be addressed as baseline security awareness training for all Information Technology personnel (system administrators, security administrators, network administrators, etc.):

1. Protection from viruses, worms, Trojan horses, and other malicious code—scanning, updating definitions.
2. Data backup and storage—centralized or decentralized approach.
3. Timely application of system patches—part of configuration management.
4. Access control measures.
5. Network infrastructure protection measures.

5.2.2 Security Training Records

Records of individual basic security awareness training and specific information system security training shall be documented, kept current, and maintained by the CSO/SIB/Compact Officer. Maintenance of training records can be delegated to the local level.

5.2.3 References/Citations/Directives

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

Figure 4 – Security Awareness Training Implemented by a Local Police Department

A local police department with a staff of 20 sworn law-enforcement officers and 15 support personnel worked with a vendor to develop role-specific security-awareness training, and required all staff to complete this training upon assignment and every two years thereafter. The local police department scheduled the sworn law-enforcement training to coincide with their NCIC certification training. The vendor maintained the training records for the police department's entire staff, and provided reporting to the department to help it ensure compliance with the CJIS Security Policy.

5.3 Policy Area 3: Incident Response

There has been an increase in the number of accidental or malicious computer attacks against both government and private agencies, regardless of whether the systems are high or low profile. Agencies shall: (i) establish an operational incident handling capability for agency information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; (ii) track, document, and report incidents to appropriate agency officials and/or authorities.

ISOs have been identified as the POC on security-related issues for their respective agencies and shall ensure LASOs institute the CSA incident response reporting procedures at the local level. Appendix F contains a sample incident notification letter for use when communicating the details of an incident to the FBI CJIS ISO.

Refer to Section 5.13.5 for additional incident response requirements related to mobile devices used to access CJI.

5.3.1 Reporting Information Security Events

The agency shall promptly report incident information to appropriate authorities. Information security events and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken. Formal event reporting and escalation procedures shall be in place. Wherever feasible, the agency shall employ automated mechanisms to assist in the reporting of security incidents. All employees, contractors and third party users shall be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of agency assets and are required to report any information security events and weaknesses as quickly as possible to the designated point of contact.

5.3.1.1 Reporting Structure and Responsibilities

5.3.1.1.1 FBI CJIS Division Responsibilities

The FBI CJIS Division shall:

1. Manage and maintain the CJIS Division's Computer Security Incident Response Capability (CSIRC).
2. Serve as a central clearinghouse for all reported intrusion incidents, security alerts, bulletins, and other security-related material.
3. Ensure additional resources for all incidents affecting FBI CJIS Division controlled systems as needed.
4. Disseminate prompt advisories of system threats and operating system vulnerabilities via the security policy resource center on FBI.gov, to include but not limited to: Product Security Bulletins, Virus Bulletins, and Security Clips.
5. Track all reported incidents and/or trends.
6. Monitor the resolution of all incidents.

5.3.1.1.2 CSA ISO Responsibilities

The CSA ISO shall:

1. Assign individuals in each state, federal, and international law enforcement organization to be the primary point of contact for interfacing with the FBI CJIS Division concerning incident handling and response.
2. Identify individuals who are responsible for reporting incidents within their area of responsibility.
3. Collect incident information from those individuals for coordination and sharing among other organizations that may or may not be affected by the incident.
4. Develop, implement, and maintain internal incident response procedures and coordinate those procedures with other organizations that may or may not be affected.
5. Collect and disseminate all incident-related information received from the Department of Justice (DOJ), FBI CJIS Division, and other entities to the appropriate local law enforcement POCs within their area.
6. Act as a single POC for their jurisdictional area for requesting incident response assistance.

5.3.2 Management of Information Security Incidents

A consistent and effective approach shall be applied to the management of information security incidents. Responsibilities and procedures shall be in place to handle information security events and weaknesses effectively once they have been reported.

5.3.2.1 Incident Handling

The agency shall implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. Wherever feasible, the agency shall employ automated mechanisms to support the incident handling process.

Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. The agency should incorporate the lessons learned from ongoing incident handling activities into the incident response procedures and implement the procedures accordingly.

5.3.2.2 Collection of Evidence

Where a follow-up action against a person or agency after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

5.3.3 Incident Response Training

The agency shall ensure general incident response roles responsibilities are included as part of required security awareness training.

5.3.4 Incident Monitoring

The agency shall track and document information system security incidents on an ongoing basis. The CSA ISO shall maintain completed security incident reporting forms until the subsequent FBI triennial audit or until legal action (if warranted) is complete; whichever time-frame is greater.

5.3.5 References/Citations/Directives

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

Figure 5 – Incident Response Process Initiated by an Incident in a Local Police Department

A state ISO received a notification from a local police department that suspicious network activity from a known botnet was detected on their network. The state ISO began the process of collecting all pertinent information about this incident, e.g. incident date/time, points-of-contact, systems affected, nature of the incident, actions taken, etc. and requested that the local police department confirm that their malware signatures were up to date. The state ISO contacted both the FBI CJIS ISO and state CSO to relay the preliminary details of this incident. The FBI CJIS ISO instructed the involved parties to continue their investigation and to submit an incident response form once all the information had been gathered. The FBI CJIS ISO contacted the lead for the FBI CSIRC to inform them that an incident response form was forthcoming. The state ISO gathered the remainder of the information from the local police department and submitted a completed incident response form to the FBI CJIS ISO who subsequently provided it to the FBI CSIRC. The FBI CSIRC notified the Department of Justice Computer Incident Response Team (DOJCIRT). The state ISO continued to monitor the situation, passing relevant details to the FBI CJIS ISO, ultimately determining that the botnet was eliminated from the local police department's infrastructure. Subsequent investigations determined that the botnet was restricted to the department's administrative infrastructure and thus no CJI was compromised.

5.4 Policy Area 4: Auditing and Accountability

Agencies shall implement audit and accountability controls to increase the probability of authorized users conforming to a prescribed pattern of behavior. Agencies shall carefully assess the inventory of components that compose their information systems to determine which security controls are applicable to the various components.

Auditing controls are typically applied to the components of an information system that provide auditing capability (servers, etc.) and would not necessarily be applied to every user-level workstation within the agency. As technology advances, more powerful and diverse functionality can be found in such devices as personal digital assistants and cellular telephones, which may require the application of security controls in accordance with an agency assessment of risk.

Refer to Section 5.13.6 for additional audit requirements related to mobile devices used to access CJI.

5.4.1 Auditable Events and Content (Information Systems)

The agency's information system shall generate audit records for defined events. These defined events include identifying significant events which need to be audited as relevant to the security of the information system. The agency shall specify which information system components carry out auditing activities. Auditing activity can affect information system performance and this issue must be considered as a separate factor during the acquisition of information systems.

The agency's information system shall produce, at the application and/or operating system level, audit records containing sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. The agency shall periodically review and update the list of agency-defined auditable events. In the event an agency does not use an automated system, manual recording of activities shall still take place.

5.4.1.1 Events

The following events shall be logged:

1. Successful and unsuccessful system log-on attempts.
2. Successful and unsuccessful attempts to use:
 - a. access permission on a user account, file, directory or other system resource;
 - b. create permission on a user account, file, directory or other system resource;
 - c. write permission on a user account, file, directory or other system resource;
 - d. delete permission on a user account, file, directory or other system resource;
 - e. change permission on a user account, file, directory or other system resource.
3. Successful and unsuccessful attempts to change account passwords.
4. Successful and unsuccessful actions by privileged accounts.
5. Successful and unsuccessful attempts for users to:

- a. access the audit log file;
- b. modify the audit log file;
- c. destroy the audit log file.

5.4.1.1.1 Content

The following content shall be included with every audited event:

- 1. Date and time of the event.
- 2. The component of the information system (e.g., software component, hardware component) where the event occurred.
- 3. Type of event.
- 4. User/subject identity.
- 5. Outcome (success or failure) of the event.

5.4.2 Response to Audit Processing Failures

The agency's information system shall provide alerts to appropriate agency officials in the event of an audit processing failure. Audit processing failures include, for example: software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

5.4.3 Audit Monitoring, Analysis, and Reporting

The responsible management official shall designate an individual or position to review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, to report findings to appropriate officials, and to take necessary actions. Audit review/analysis shall be conducted at a minimum once a week. The frequency of review/analysis should be increased when the volume of an agency's processing indicates an elevated need for audit review. The agency shall increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to agency operations, agency assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

5.4.4 Time Stamps

The agency's information system shall provide time stamps for use in audit record generation. The time stamps shall include the date and time values generated by the internal system clocks in the audit records. The agency shall synchronize internal information system clocks on an annual basis.

5.4.5 Protection of Audit Information

The agency's information system shall protect audit information and audit tools from modification, deletion and unauthorized access.

5.4.6 Audit Record Retention

The agency shall retain audit records for at least one (1) year. Once the minimum retention time period has passed, the agency shall continue to retain audit records until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions.

5.4.7 Logging NCIC and III Transactions

A log shall be maintained for a minimum of one (1) year on all NCIC and III transactions. The III portion of the log shall clearly identify both the operator and the authorized receiving agency. III logs shall also clearly identify the requester and the secondary recipient. The identification on the log shall take the form of a unique identifier that shall remain unique to the individual requester and to the secondary recipient throughout the minimum one year retention period.

5.4.8 References/Citations/Directives

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

Figure 6 – Local Police Department's Use of Audit Logs

A state CSO contacted a local police department regarding potentially inappropriate use of CHRI that was retrieved using the local department's ORI. The state CSO requested all relevant information from the police department to reconcile state NCIC and III logs against local police department logs. The police department provided the combination of their CJI processing application's logs with relevant operating system and network infrastructure logs to help verify the identity of the users conducting these queries. The review of these logs substantiated the CSO's suspicion.

5.5 Policy Area 5: Access Control

Access control provides the planning and implementation of mechanisms to restrict reading, writing, processing and transmission of CJIS information and the modification of information systems, applications, services and communication configurations allowing access to CJIS information.

Refer to Section 5.13.7 for additional access control requirements related to mobile devices used to access CJI.

5.5.1 Account Management

The agency shall manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The agency shall validate information system accounts at least annually and shall document the validation process. The validation and documentation of accounts can be delegated to local agencies.

Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. The agency shall identify authorized users of the information system and specify access rights/privileges. The agency shall grant access to the information system based on:

1. Valid need-to-know/need-to-share that is determined by assigned official duties.
2. Satisfaction of all personnel security criteria.

The agency responsible for account creation shall be notified when:

1. A user's information system usage or need-to-know or need-to-share changes.
2. A user is terminated or transferred or associated accounts are removed, disabled, or otherwise secured.

5.5.2 Access Enforcement

The information system shall enforce assigned authorizations for controlling access to the system and contained information. The information system controls shall restrict access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel.

Explicitly authorized personnel include, for example, security administrators, system and network administrators, and other privileged users with access to system control, monitoring, or administration functions (e.g., system administrators, information system security officers, maintainers, system programmers).

Access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) shall be employed by agencies to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system.

5.5.2.1 Least Privilege

The agency shall approve individual access privileges and shall enforce physical and logical access restrictions associated with changes to the information system; and generate, retain, and review records reflecting all such changes. The agency shall enforce the most restrictive set of rights/privileges or access needed by users for the performance of specified tasks. The agency shall implement least privilege based on specific duties, operations, or information systems as necessary to mitigate risk to CJI. This limits access to CJI to only authorized personnel with the need and the right to know.

Logs of access privilege changes shall be maintained for a minimum of one year or at least equal to the agency's record retention policy – whichever is greater.

5.5.2.2 System Access Control

Access control mechanisms to enable access to CJI shall be restricted by object (e.g., data set, volumes, files, records) including the ability to read, write, or delete the objects. Access controls shall be in place and operational for all IT systems to:

1. Prevent multiple concurrent active sessions for one user identification, for those applications accessing CJI, unless the agency grants authority based upon operational business needs. Agencies shall document the parameters of the operational business needs for multiple concurrent active sessions.
2. Ensure that only authorized personnel can add, change, or remove component devices, dial-up connections, and remove or alter programs.

5.5.2.3 Access Control Criteria

Agencies shall control access to CJI based on one or more of the following:

1. Job assignment or function (i.e., the role) of the user seeking access.
2. Physical location.
3. Logical location.
4. Network addresses (e.g., users from sites within a given agency may be permitted greater access than those from outside).
5. Time-of-day and day-of-week/month restrictions.

5.5.2.4 Access Control Mechanisms

When setting up access controls, agencies shall use one or more of the following mechanisms:

1. Access Control Lists (ACLs). ACLs are a register of users (including groups, machines, processes) who have been given permission to use a particular object (system resource) and the types of access they have been permitted.
2. Resource Restrictions. Access to specific functions is restricted by never allowing users to request information, functions, or other resources for which they do not have access. Three major types of resource restrictions are: menus, database views, and network devices.

3. Encryption. Encrypted information can only be decrypted, and therefore read, by those possessing the appropriate cryptographic key. While encryption can provide strong access control, it is accompanied by the need for strong key management. Follow the guidance in Section 5.10.2 for encryption requirements if encryption of stored information is employed as an access enforcement mechanism.
4. Application Level. In addition to controlling access at the information system level, access enforcement mechanisms are employed at the application level to provide increased information security for the agency.

5.5.3 Unsuccessful Login Attempts

Where technically feasible, the system shall enforce a limit of no more than 5 consecutive invalid access attempts by a user (attempting to access CJI or systems with access to CJI). The system shall automatically lock the account/node for a 10 minute time period unless released by an administrator.

5.5.4 System Use Notification

The information system shall display an approved system use notification message, before granting access, informing potential users of various usages and monitoring rules. The system use notification message shall, at a minimum, provide the following information:

1. The user is accessing a restricted information system.
2. System usage may be monitored, recorded, and subject to audit.
3. Unauthorized use of the system is prohibited and may be subject to criminal and/or civil penalties.
4. Use of the system indicates consent to monitoring and recording.

The system use notification message shall provide appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remain on the screen until the user acknowledges the notification and takes explicit actions to log on to the information system.

Privacy and security policies shall be consistent with applicable laws, executive orders, directives, policies, regulations, standards, and guidance. System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the information system. For publicly accessible systems:

- (i) the system use information is available and when appropriate, is displayed before granting access;
- (ii) any references to monitoring, recording, or auditing are in keeping with privacy accommodations for such systems that generally prohibit those activities; and
- (iii) the notice given to public users of the information system includes a description of the authorized uses of the system.

5.5.5 Session Lock

The information system shall prevent further access to the system by initiating a session lock after a maximum of 30 minutes of inactivity, and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures. Users shall directly initiate session lock mechanisms to prevent inadvertent viewing when a device is unattended. A session lock is not a substitute for logging out of the information system. In the interest of officer safety, devices that are: (1) part of a police vehicle; or (2) used to perform dispatch functions and located within a physically secure location; or (3) terminals designated solely for the purpose of receiving alert notifications (i.e. receive only terminals or ROT) used within physically secure location facilities that remain staffed when in operation, are exempt from this requirement. Note: an example of a session lock is a screen saver with password.

5.5.6 Remote Access

The agency shall authorize, monitor, and control all methods of remote access to the information system. Remote access is any temporary access to an agency's information system by a user (or an information system) communicating temporarily through an external, non-agency-controlled network (e.g., the Internet).

The agency shall employ automated mechanisms to facilitate the monitoring and control of remote access methods. The agency shall control all remote accesses through managed access control points. The agency may permit remote access for privileged functions only for compelling operational needs but shall document the rationale for such access in the security plan for the information system.

5.5.6.1 Personally Owned Information Systems

A personally owned information system shall not be authorized to access, process, store or transmit CJI unless the agency has established and documented the specific terms and conditions for personally owned information system usage. When personally owned mobile devices (i.e. bring your own device [BYOD]) are authorized, they shall be controlled in accordance with the requirements in Policy Area 13: Mobile Devices.

This control does not apply to the use of personally owned information systems to access agency's information systems and information that are intended for public access (e.g., an agency's public website that contains purely public information).

5.5.6.2 Publicly Accessible Computers

Publicly accessible computers shall not be used to access, process, store or transmit CJI. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.

5.5.7 References/Citations/Directives

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

Figure 7 – A Local Police Department’s Access Controls

A local police department purchased a new computer-assisted dispatch (CAD) system that integrated with their state CSA’s CJI interfaces. In doing so, the police department employed least-privilege practices to ensure that its employees were only given those privileges needed to perform their jobs, and as such, excluding IT administrators, employees had only non-administrative privileges on all equipment they used. The police department also used ACLs in the operating systems to control access to the CAD client’s executables. The CAD system used internal role-based access controls to ensure only those users that needed access to CJI were given it. The police department performed annual audits of user accounts on all systems under their control including remote access mechanisms, operating systems, and the CAD system to ensure all accounts were in valid states. The police department implemented authentication-failure account lockouts, system use notification via login banners, and screen-saver passwords on all equipment that processes CJI.

5.6 Policy Area 6: Identification and Authentication

The agency shall identify information system users and processes acting on behalf of users and authenticate the identities of those users or processes as a prerequisite to allowing access to agency information systems or services.

5.6.1 Identification Policy and Procedures

Each person who is authorized to store, process, and/or transmit CJI shall be uniquely identified. A unique identification shall also be required for all persons who administer and maintain the system(s) that access CJI or networks leveraged for CJI transit. The unique identification can take the form of a full name, badge number, serial number, or other unique alphanumeric identifier. Agencies shall require users to identify themselves uniquely before the user is allowed to perform any actions on the system. Agencies shall ensure that all user IDs belong to currently authorized users. Identification data shall be kept current by adding new users and disabling and/or deleting former users.

5.6.1.1 Use of Originating Agency Identifiers in Transactions and Information Exchanges

An FBI authorized originating agency identifier (ORI) shall be used in each transaction on CJIS systems in order to identify the sending agency and to ensure the proper level of access for each transaction. The original identifier between the requesting agency and the CSA/SIB/Channeler shall be the ORI, and other agency identifiers, such as user identification or personal identifier, an access device mnemonic, or the Internet Protocol (IP) address.

Agencies may act as a servicing agency and perform transactions on behalf of authorized agencies requesting the service. Servicing agencies performing inquiry transactions on behalf of another agency may do so using the requesting agency's ORI. Servicing agencies may also use their own ORI to perform inquiry transactions on behalf of a requesting agency if the means and procedures are in place to provide an audit trail for the current specified retention period. Because the agency performing the transaction may not necessarily be the same as the agency requesting the transaction, the CSA/SIB/Channeler shall ensure that the ORI for each transaction can be traced, via audit trail, to the specific agency which is requesting the transaction.

Audit trails can be used to identify the requesting agency if there is a reason to inquire into the details surrounding why an agency ran an inquiry on a subject. Agencies assigned a P (limited access) ORI shall not use the full access ORI of another agency to conduct an inquiry transaction.

5.6.2 Authentication Policy and Procedures

Authentication refers to mechanisms or processes that verify users are valid once they are uniquely identified. The CSA/SIB may develop an authentication strategy which centralizes oversight but decentralizes the establishment and daily administration of the security measures for access to CJI.

Each individual's identity shall be authenticated at either the local agency, CSA, SIB or Channeler level. The authentication strategy shall be part of the agency's audit for policy compliance. The FBI CJIS Division shall identify and authenticate all individuals who establish

direct web-based interactive sessions with FBI CJIS Services. The FBI CJIS Division shall authenticate the ORI of all message-based sessions between the FBI CJIS Division and its customer agencies but will not further authenticate the user nor capture the unique identifier for the originating operator because this function is performed at the local agency, CSA, SIB or Channeler level.

5.6.2.1 Standard Authenticators

Authenticators are (the something you know, something you are, or something you have) part of the identification and authentication process. Examples of standard authenticators include passwords, tokens, biometrics, and personal identification numbers (PIN). Users shall not be allowed to use the same password or PIN in the same logon sequence.

5.6.2.1.1 Password

Agencies shall follow the secure password attributes, below, to authenticate an individual's unique ID. Passwords shall:

1. Be a minimum length of eight (8) characters on all systems.
2. Not be a dictionary word or proper name.
3. Not be the same as the Userid.
4. Expire within a maximum of 90 calendar days.
5. Not be identical to the previous ten (10) passwords.
6. Not be transmitted in the clear outside the secure location.
7. Not be displayed when entered.

5.6.2.1.2 Personal Identification Number (PIN)

When agencies implement the use of a PIN as a standard authenticator, the PIN attributes shall follow the guidance in section 5.6.2.1.1 (password). When agencies utilize a PIN in conjunction with a certificate or a token (e.g. key fob with rolling numbers) for the purpose of advanced authentication, agencies shall follow the PIN attributes described below. For example: A user certificate is installed on a smartphone for the purpose of advanced authentication (AA). As the user invokes that certificate, a PIN meeting the below attributes shall be used to access the certificate for the AA process.

1. Be a minimum of six (6) digits
2. Have no repeating digits (i.e., 112233)
3. Have no sequential patterns (i.e., 123456)
4. Not be the same as the Userid.
5. Expire within a maximum of 365 calendar days.
 - a. If a PIN is used to access a soft certificate which is the second factor of authentication, AND the first factor is a password that complies with the requirements in Section 5.6.2.1.1, then the 365 day expiration requirement can be waived by the CSO.

6. Not be identical to the previous three (3) PINs.
7. Not be transmitted in the clear outside the secure location.
8. Not be displayed when entered.

EXCEPTION: When a PIN is used for local device authentication, the only requirement is that it be a minimum of six (6) digits.

5.6.2.2 Advanced Authentication

Advanced Authentication (AA) provides for additional security to the typical user identification and authentication of login ID and password, such as: biometric systems, user-based public key infrastructure (PKI), smart cards, software tokens, hardware tokens, paper (inert) tokens, or “Risk-based Authentication” that includes a software token element comprised of a number of factors, such as network information, user information, positive device identification (i.e. device forensics, user pattern analysis and user binding), user profiling, and high-risk challenge/response questions.

5.6.2.2.1 Advanced Authentication Policy and Rationale

The requirement to use or not use AA is dependent upon the physical, personnel, and technical security controls associated with the user location and whether CJI is accessed directly or indirectly. AA shall not be required for users requesting access to CJI from within the perimeter of a physically secure location (Section 5.9), when the technical security controls have been met (Sections 5.5 and 5.10), or when the user has no ability to conduct transactional activities on state and national repositories, applications, or services (i.e. indirect access). Conversely, if the technical security controls have not been met, AA shall be required even if the request for CJI originates from within a physically secure location. Section 5.6.2.2.2 provides agencies with a decision tree to help guide AA decisions. The CSO will make the final determination of whether access is considered indirect.

The intent of AA is to meet the standards of two-factor authentication. Two-factor authentication employs the use of two of the following three factors of authentication: something you know (e.g. password), something you have (e.g. hard token), something you are (e.g. biometric). The two authentication factors shall be unique (i.e. password/token or biometric/password but not password/password or token/token).

CSO approved compensating controls to meet the AA requirement on agency-issued smartphones, tablets, and iPads are permitted. Compensating controls are temporary control measures that are implemented in lieu of the required AA control measures when an agency cannot meet a requirement due to legitimate technical or business constraints. The compensating controls shall:

1. Meet the intent of the CJIS Security Policy AA requirement
2. Provide a similar level of protection or security as the original AA requirement
3. Not rely upon the existing requirements for AA as compensating controls

Mobile Device Management (MDM) must be implemented and provide at least two of the other examples of compensating controls listed below.

Additionally, compensating controls may rely upon other, non-AA, existing requirements as compensating controls and/or be combined with new controls to create compensating controls.

The proposed compensating controls for AA are a combination of controls that provide acceptable assurance it is the authorized user authenticating and not an impersonator or (in the case of agency-issued device used by multiple users) controls that reduce the risk of exposure if information is accessed by an unauthorized party.

Examples of AA compensating controls for and agency-issued smartphones and tablets are:

- Possession of the agency issued smartphone, tablet, or iPad as an indication it is the authorized user
- Implemented password protection on the Mobile Device Management application and/or secure container where the authentication application is stored
- Enable remote device locking
- Enable remote data deletion
- Enable automatic data wipe after predetermined number of failed authentication attempts
- Remote device location (GPS) tracking
- Require CJIS Security Policy compliant password to access the device
- Use of device certificates

INTERIM COMPLIANCE:

1. Internet Protocol Security (IPSec) does not meet the 2011 requirements for advanced authentication; however, agencies that have funded/implemented IPSec in order to meet the AA requirements of CJIS Security Policy v.4.5 may continue to utilize IPSec for AA until September 30, 2014. Examples:
 - a. A police officer runs a query for CJI from his/her laptop mounted in a police vehicle. The police officer leverages a cellular network as the transmission medium; authenticates the device using IPSec key exchange; and tunnels across the cellular network using the IPSec virtual private network (VPN). IPSec was funded and installed in order to meet the AA requirements of CJIS Security Policy version 4.5. AA requirements are waived until September 30, 2014.
 - b. A detective accesses CJI from various locations while investigating a crime scene. The detective uses an agency managed laptop with IPSec installed and leverages a cellular network as the transmission medium. IPSec was funded and installed in order to meet the AA requirements of CJIS Security Policy version 4.5. AA requirements are waived until September 30, 2014.

EXCEPTION:

AA shall be required when the requested service has built AA into its processes and requires a user to provide AA before granting access. EXAMPLES:

- a. A user, irrespective of his/her location, accesses the LEO website. The LEO has AA built into its services and requires AA prior to granting access. AA is required.
- b. A user, irrespective of their location, accesses a State's portal through which access to CJI is facilitated. The State Portal has AA built into its processes and requires AA prior to granting access. AA is required.

5.6.2.2.2 Advanced Authentication Decision Tree

The following AA Decision Tree, coupled with figures 9 and 10 below, assists decision makers in determining whether or not AA is required.

1. Can request's originating location be determined physically?

If either (a) or (b) below are true the answer to the above question is "yes". Proceed to question 2.

- a. The IP address is attributed to a physical structure; or
- b. The mnemonic is attributed to a specific device assigned to a specific location that is a physical structure.

If neither (a) or (b) above are true then the answer is "no". Skip to question number 4.

2. Does request originate from within a physically secure location as described in Section 5.9.1?

If either (a) or (b) below are true the answer to the above question is "yes". Proceed to question 3.

- a. The IP address is attributed to a physically secure location; or
- b. If a mnemonic is used it is attributed to a specific device assigned to a specific physically secure location.

If neither (a) or (b) above are true then the answer is "no". Decision tree completed. AA required.

3. Are all required technical controls implemented at this location or at the controlling agency?

If either (a) or (b) below are true the answer to the above question is "yes". Decision tree completed. AA requirement waived.

- a. Appropriate technical controls listed in Sections 5.5 and 5.10 are implemented; or
- b. The controlling agency (i.e. parent agency or agency leveraged as conduit to CJI) extends its wide area network controls down to the requesting agency and the extended controls provide assurance equal or greater to the controls listed in Sections 5.5 and 5.10.

If neither (a) or (b) above are true then the answer is "no". Decision tree completed. AA required.

4. Does request originate from an agency-managed user device?

If either (a) or (b) below are true the answer to the above question is “yes”. Proceed to question 5.

- a. The static IP address or MAC address can be traced to registered device; or
- b. Certificates are issued to agency managed devices only and certificate exchange is allowed only between authentication server and agency issued devices.

If neither (a) or (b) above are true then the answer is “no”. Decision tree completed. AA required.

5. Is the agency managed user device associated with and located within a law enforcement conveyance?

If any of the (a), (b), or (c) statements below is true the answer to the above question is “yes”. Proceed to Figure 9 Step 3.

- a. The static IP address or MAC address is associated with a device associated with a law enforcement conveyance; or
- b. The certificate presented is associated with a device associated with a law enforcement conveyance; or
- c. The mnemonic presented is associated with a specific device assigned and that device is attributed to a law enforcement conveyance.

If none of the (a), (b), or (c) statements above are true then the answer is “no”. Skip to question number 7.

6. Is the user device an agency-issued and controlled smartphone or tablet?

If both (a) and (b) below are true, the answer to the above question is “yes.” Proceed to question number 7.

- a. The law enforcement agency issued the device to an individual; and
- b. The device is subject to administrative management control of the issuing agency.

If either (a) or (b) above is false, then the answer is “no.” Decision tree completed. AA required.

7. Does the agency-issued smartphone have CSO-approved AA compensating controls implemented?

If (a) and (b) below are true, the answer to the above question is “yes.” Decision tree completed. AA requirement is waived.

- a. An agency cannot meet a requirement due to legitimate technical or business constraints; and
- b. The CSO has given written approval permitting AA compensating controls to be implemented in lieu of the required AA control measures.

If either (a) or (b) above is false then the answer is “no.” Decision tree completed. AA required.

5.6.3 Identifier and Authenticator Management

The agency shall establish identifier and authenticator management processes.

5.6.3.1 Identifier Management

In order to manage user identifiers, agencies shall:

1. Uniquely identify each user.
2. Verify the identity of each user.
3. Receive authorization to issue a user identifier from an appropriate agency official.
4. Issue the user identifier to the intended party.
5. Disable the user identifier after a specified period of inactivity.
6. Archive user identifiers.

5.6.3.2 Authenticator Management

In order to manage information system authenticators, agencies shall:

1. Define initial authenticator content.
2. Establish administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators.
3. Change default authenticators upon information system installation.
4. Change/refresh authenticators periodically.

Information system authenticators include, for example, tokens, user-based PKI certificates, biometrics, passwords, and key cards. Users shall take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and immediately reporting lost or compromised authenticators.

5.6.4 Assertions

Identity providers can be leveraged to identify individuals and assert the individual’s identity to a service or to a trusted broker who will in-turn assert the identity to a service. Assertion mechanisms used to communicate the results of a remote authentication to other parties shall be:

1. Digitally signed by a trusted entity (e.g., the identity provider).
2. Obtained directly from a trusted entity (e.g. trusted broker) using a protocol where the trusted entity authenticates to the relying party using a secure protocol (e.g. transport layer security [TLS]) that cryptographically authenticates the verifier and protects the assertion.

Assertions generated by a verifier shall expire after 12 hours and shall not be accepted thereafter by the relying party.

5.6.5 References/Citations/Directives

Appendix C contains all of the references used in this Policy and may contain additional sources that apply to this section.

Figure 8 – Advanced Authentication Use Cases

Use Case 1 - A Local Police Department Authentication Control Scenario

During the course of an investigation, a detective attempts to access Criminal Justice Information (CJI) from a hotel room using an agency issued mobile broadband card. To gain access, the detective first establishes the remote session via a secure virtual private network (VPN) tunnel (satisfying the requirement for encryption). Upon connecting to the agency network, the detective is challenged for a username (identification), password (“something you know”), and a one-time password OTP (“something you have”) from a hardware token to satisfy the requirement for advanced authentication. Once the detective’s credentials are validated, his identity is asserted by the infrastructure to all authorized applications needed to complete his queries.

Use Case 2 – Use of a Smart Card

A user is issued a smart card that is loaded with user-specific digital certificates from a terminal within a controlled area. The user selects an application that will provide access to Criminal Justice Information (CJI) then enters the proper username (identification) and password (“something you know”). Once prompted, the user connects the smart card (“something you have”) to the terminal. The user is prompted to enter a personal identification number (PIN) to unlock the smart card. Once unlocked, the smart card sends the certificates to the authentication management server at the local agency where the combined username, password, and digital user certificates are validated. The user has satisfied the requirement for AA and is granted access to CJI.

Use Case 3 – Out of Band One-Time-Password (OTP) – Mobile phone-based

Using an agency- issued laptop, a user connects to the agency network via an agency-issued mobile broadband card and an encrypted virtual private network (VPN) tunnel. As part of an on-going investigation, the user initiates an application that will permit access to Criminal Justice Information (CJI). The user is prompted to enter a username (identification) and a password (“something you know”). Once that has been completed, a text message containing a one-time password (OTP) is sent via text message (out of band) to the user’s agency-issued cell phone. The user is challenged via the CJI application for that OTP. The user enters the OTP (“something you have”) then the username, password, and OTP are validated. The user has satisfied the requirement for AA and is granted access to CJI.

Use Case 4 – Improper Use of a One-Time-Password (OTP) – Laptop

Using an agency- issued laptop, a user connects to the agency network via an agency-issued mobile broadband card and an encrypted virtual private network (VPN) tunnel. As part of an on-going investigation, the user initiates an application that will permit access to Criminal Justice Information (CJI). The user is prompted to enter a username (identification) and a password (“something you know”). Once that has been completed, a one-time password (OTP) is sent to the user’s agency-issued laptop (in band) via pop-up message. The user is challenged via the CJI application for that OTP; however, the delivery of the OTP to the device that is being used to access CJI (in band) defeats the purpose of the second factor. This method does not satisfy the requirement for AA, and therefore the user should not be granted access to CJI. See the below explanation:

This method of receiving the necessary OTP (in band) does not guarantee the authenticity of the user’s identity because anyone launching the CJI application and entering a valid username/password combination is presented the OTP via a pop-up which is intend to be the second factor of authentication. This method makes the application accessible to anyone with knowledge of the valid username and password. Potentially, this is no more secure than using only a single factor of authentication.

Use Case 5 – Risk-based Authentication (RBA) Implementation

A user has moved office locations and requires email access (containing Criminal Justice Information) via an Outlook Web Access (OWA) client utilizes a risk-based authentication (RBA) solution. The user launches the OWA client and is prompted to enter a username (identification) and a password (“something you know”). The RBA detects this computer has not previously been used by the user, is not listed under the user’s profile, and then presents high-risk challenge/response question(s) which the user is prompted to answer. Once the questions have been verified as correct, the user is authenticated and granted access to the email. Meanwhile, the RBA logs and collects a number of device forensic information and captures the user pattern analysis to update the user’s profile. The CJIS Security Policy requirements for RBA have been satisfied.

Use Case 6 – Improper Risk-based Authentication (RBA) Implementation

A user has moved office locations and requires access to email containing Criminal Justice Information (CJI) via an Outlook Web Access (OWA) client utilizing a risk-based authentication (RBA) solution. The user launches the OWA client and is prompted to enter a username (identification) and a password (“something you know”). The RBA detects this computer has not previously been used by the user and is not listed under the user’s profile. The user is prompted to answer high-risk challenge/response questions for verification and authorization to access to the email; however, if the second authentication factor is to answer additional questions presented every time the user logs on, then this solution is referred to as a knowledge-based authentic on (KBA) solution. A KBA solution does not satisfy the requirement for AA, and therefore the user should not be granted access to CJI.

See the below explanation:

A KBA solution is not a viable advanced authentication (AA) solution per the CJIS Security Policy (CSP). The KBA asks questions and compares the answers to those stored within the user's profile. A KBA is neither a CSP compliant two factor authentication solution, nor does it meet the CSP criteria of a risk-based authentication (RBA) solution which logs and collects a number of device forensic information and captures the user pattern analysis to update the user's profile. Using this collected data, the RBA presents challenge/response questions when changes to the user's profile are noted versus every time the user logs in.

Use Case 7 – Advanced Authentication Compensating Controls on Agency-Issued Smartphones

An authorized user is issued a smartphone that is administratively managed by the agency-installed mobile device management (MDM) solution to ensure device compliance with the CJIS Security Policy. The user initiates an email client on the smartphone that contains emails with CJI. The email client challenges the user to enter a username (identification) and a password (one factor: something you know) which are forwarded to the local agency for authentication. The smartphone lacks the technical capability to challenge the user for a second factor of authentication. This email client is used across the state agency so access is a necessity for the user's job functions.

An audit by the CSA identifies the agency's use of the agency smartphone as not compliant with AA requirements due to the authorized user authenticating with only one factor instead of the required two factors.

Subsequently, the agency performs a risk assessment of their smartphone authentication solution and document a legitimate technical constraint due to the lack of technical solutions for smartphone-based two-factor authentication. The risk assessment identifies the following compensating controls that, when combined with the authorized user authenticating to the local agency with their password, meet the intent of the AA requirement by providing a similar level of security:

1. Enhance smartphone policy to enable possession of the smartphone to be considered a factor of authentication (i.e. something you have). Require authorized users to treat the smartphone as a controlled device and protect it as they would a personal credit card or an issued firearm to ensure only they will be in possession of the device
2. Move the email client used to authenticate with the local agency inside an encrypted, password-protected secure container on the smartphone ensuring only the authorized user can access the email application to authenticate.

The agency submits an AA compensating controls request to the CSO outlining the technical constraint identified by the risk assessment, what compensating controls will be employed, and the desired duration of the compensating controls.

The CSO approves the agency's request and provides documentation of the approval to the agency to maintain for audit purposes. The agency enacts the compensating controls and informs agency personnel they are permitted to access CJI via the agency-issued smartphone.

Figure 9 – Authentication Decision for Known Location

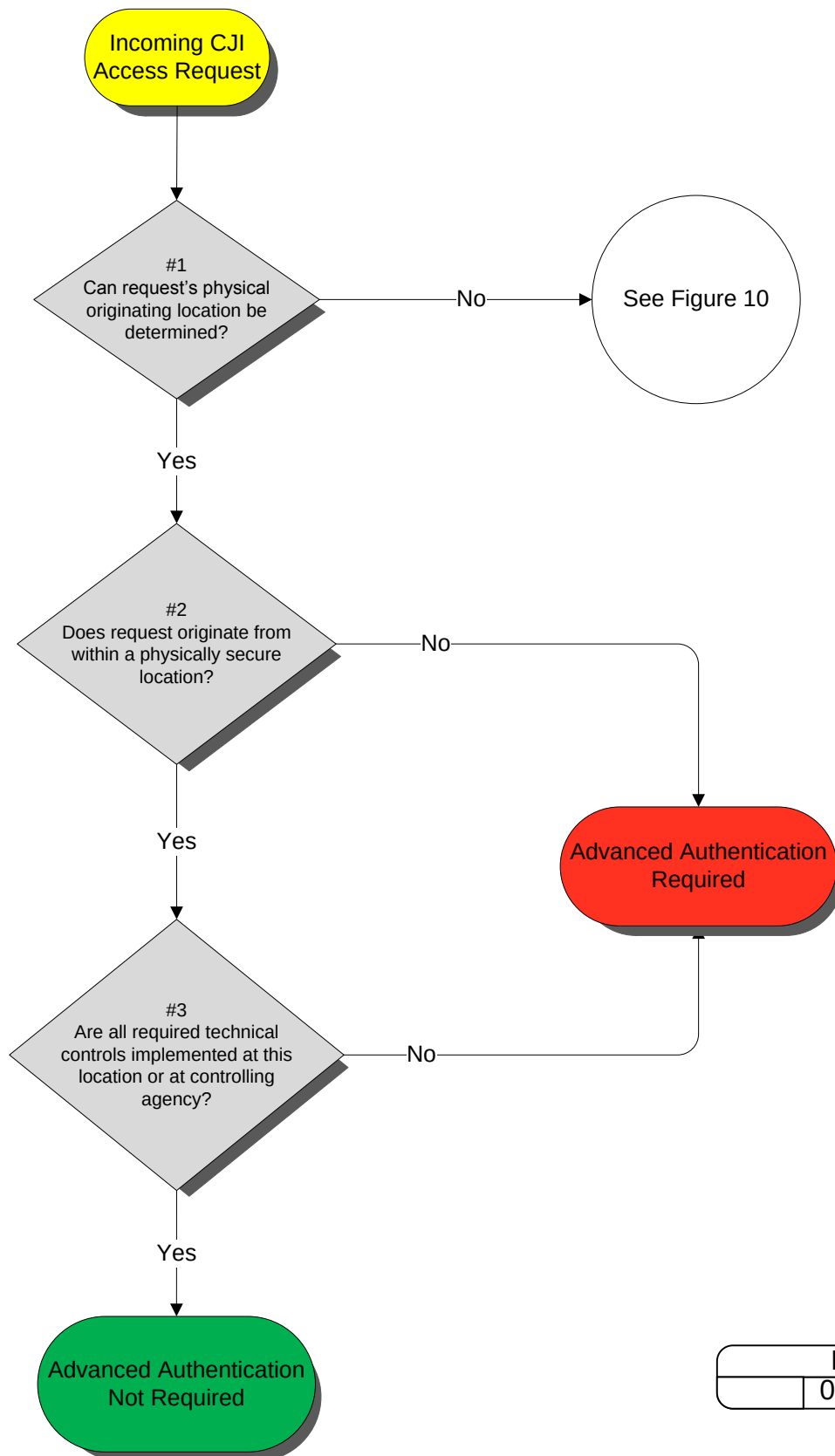


Figure 9		
	08/04/2014	

Figure 10 – Authentication Decision for Unknown Location

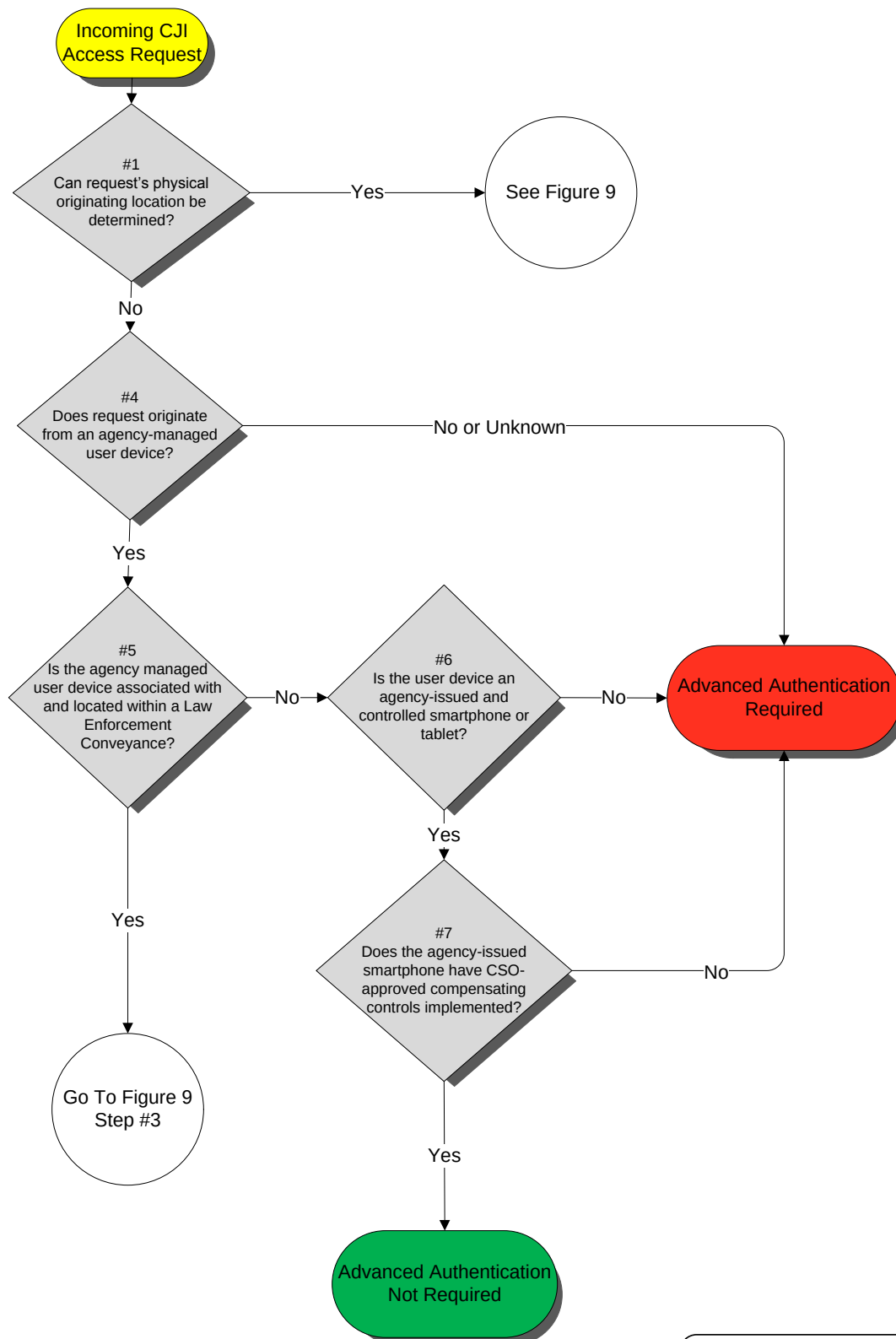


Figure 10		
	08/04/2014	

5.7 Policy Area 7: Configuration Management

5.7.1 Access Restrictions for Changes

Planned or unplanned changes to the hardware, software, and/or firmware components of the information system can have significant effects on the overall security of the system. The goal is to allow only qualified and authorized individuals access to information system components for purposes of initiating changes, including upgrades, and modifications. Section 5.5, Access Control, describes agency requirements for control of privileges and restrictions.

5.7.1.1 Least Functionality

The agency shall configure the application, service, or information system to provide only essential capabilities and shall specifically prohibit and/or restrict the use of specified functions, ports, protocols, and/or services.

5.7.1.2 Network Diagram

The agency shall ensure that a complete topological drawing depicting the interconnectivity of the agency network, to criminal justice information, systems and services is maintained in a current status. See Appendix C for sample network diagrams.

The network topological drawing shall include the following:

1. All communications paths, circuits, and other components used for the interconnection, beginning with the agency-owned system(s) and traversing through all interconnected systems to the agency end-point.
2. The logical location of all components (e.g., firewalls, routers, switches, hubs, servers, encryption devices, and computer workstations). Individual workstations (clients) do not have to be shown; the number of clients is sufficient.
3. “For Official Use Only” (FOUO) markings.
4. The agency name and date (day, month, and year) drawing was created or updated.

5.7.2 Security of Configuration Documentation

The system configuration documentation often contains sensitive details (e.g. descriptions of applications, processes, procedures, data structures, authorization processes, data flow, etc.) Agencies shall protect the system documentation from unauthorized access consistent with the provisions described in Section 5.5 Access Control.

5.7.3 References/Citations/Directives

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

Figure 11 – A Local Police Department’s Configuration Management Controls

A local police department decided to update their CAD system, and in doing so tracked all changes made to their infrastructure in a configuration management journal, updated their network topology documents to include all new components in their architecture, then marked all documentation as FOUO and stored them securely.

5.8 Policy Area 8: Media Protection

Media protection policy and procedures shall be documented and implemented to ensure that access to electronic and physical media in all forms is restricted to authorized individuals. Procedures shall be defined for securely handling, transporting and storing media.

5.8.1 Media Storage and Access

The agency shall securely store electronic and physical media within physically secure locations or controlled areas. The agency shall restrict access to electronic and physical media to authorized individuals. If physical and personnel restrictions are not feasible then the data shall be encrypted per Section 5.10.1.2.

5.8.2 Media Transport

The agency shall protect and control electronic and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel.

5.8.2.1 Digital Media during Transport

Controls shall be in place to protect digital media containing CJI while in transport (physically moved from one location to another) to help prevent compromise of the data. Encryption, as defined in Section 5.10.1.2 of this Policy, is the optimal control during transport; however, if encryption of the data isn't possible then each agency shall institute physical controls to ensure the security of the data.

5.8.2.2 Physical Media in Transit

The controls and security measures in this document also apply to CJI in physical (printed documents, printed imagery, etc.) form. Physical media shall be protected at the same level as the information would be protected in electronic form.

5.8.3 Electronic Media Sanitization and Disposal

The agency shall sanitize, that is, overwrite at least three times or degauss electronic media prior to disposal or release for reuse by unauthorized individuals. Inoperable electronic media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel.

5.8.4 Disposal of Physical Media

Physical media shall be securely disposed of when no longer required, using formal procedures. Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information compromise by unauthorized individuals. Physical media shall be destroyed by shredding or incineration. Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel.

5.8.5 References/Citations/Directives

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

Figure 12 – A Local Police Department’s Media Management Policies

A local police department implemented a replacement CAD system that integrated to their state’s CSA and was authorized to process CJI. The police department contracted with an off-site media manager to store backups of their data in the contractor’s vaults, but the contractor was not authorized to process or store CJI. To ensure the confidentiality of the police department’s data while outside its perimeter, they encrypted all data going to the contractor with an encryption product that is FIPS 140-2 certified. The police department rotated and reused media through the contractor’s vaults periodically, and when it required destruction, the police department incinerated the media to irreversibly destroy any data on it.

5.9 Policy Area 9: Physical Protection

Physical protection policy and procedures shall be documented and implemented to ensure CJI and information system hardware, software, and media are physically protected through access control measures.

5.9.1 Physically Secure Location

A physically secure location is a facility, a police vehicle, or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems. The physically secure location is subject to criminal justice agency management control; SIB control; FBI CJIS Security addendum; or a combination thereof.

Sections 5.9.1.1 – 5.9.1.8 describe the physical controls required in order to be considered a physically secure location, while Section 5.12 describes the minimum personnel security controls required for unescorted access to a physically secure location. Sections 5.5, 5.6.2.2.1, and 5.10 describe the requirements for technical security controls required to access CJI from within the perimeter of a physically secure location without AA.

5.9.1.1 Security Perimeter

The perimeter of a physically secure location shall be prominently posted and separated from non-secure locations by physical controls. Security perimeters shall be defined, controlled and secured in a manner acceptable to the CSA or SIB.

5.9.1.2 Physical Access Authorizations

The agency shall develop and keep current a list of personnel with authorized access to the physically secure location (except for those areas within the permanent facility officially designated as publicly accessible) or shall issue credentials to authorized personnel.

5.9.1.3 Physical Access Control

The agency shall control all physical access points (except for those areas within the facility officially designated as publicly accessible) and shall verify individual access authorizations before granting access.

5.9.1.4 Access Control for Transmission Medium

The agency shall control physical access to information system distribution and transmission lines within the physically secure location.

5.9.1.5 Access Control for Display Medium

The agency shall control physical access to information system devices that display CJI and shall position information system devices in such a way as to prevent unauthorized individuals from accessing and viewing CJI.

5.9.1.6 Monitoring Physical Access

The agency shall monitor physical access to the information system to detect and respond to physical security incidents.

5.9.1.7 Visitor Control

The agency shall control physical access by authenticating visitors before authorizing escorted access to the physically secure location (except for those areas designated as publicly accessible). The agency shall escort visitors at all times and monitor visitor activity.

5.9.1.8 Delivery and Removal

The agency shall authorize and control information system-related items entering and exiting the physically secure location.

5.9.2 Controlled Area

If an agency cannot meet all of the controls required for establishing a physically secure location, but has an operational need to access or store CJI, the agency shall designate an area, a room, or a storage container, as a controlled area for the purpose of day-to-day CJI access or storage. The agency shall, at a minimum:

1. Limit access to the controlled area during CJI processing times to only those personnel authorized by the agency to access or view CJI.
2. Lock the area, room, or storage container when unattended.
3. Position information system devices and documents containing CJI in such a way as to prevent unauthorized individuals from access and view.
4. Follow the encryption requirements found in Section 5.10.1.2 for electronic storage (i.e. data “at rest”) of CJI.

5.9.3 References/Citations/Directives

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

Figure 13 – A Local Police Department's Physical Protection Measures

A local police department implemented a replacement CAD system that was authorized to process CJI over an encrypted VPN tunnel to the state's CSA. The police department established a physically separated wing within their precinct separated by locked doors, walls, and a monitored security system within which CJI was processed by dispatchers, officers, and detectives. Only those persons with the appropriate authorizations were permitted within this wing unless accompanied by such a person. Within this secure wing the police department further segregated the back-office information systems' infrastructure within a separately controlled area restricted only to those authorized administrative personnel with a need to enter.

5.10 Policy Area 10: System and Communications Protection and Information Integrity

Examples of systems and communications safeguards range from boundary and transmission protection to securing an agency's virtualized environment. In addition, applications, services, or information systems must have the capability to ensure system integrity through the detection and protection against unauthorized changes to software and information. This section details the policy for protecting systems and communications infrastructures.

Refer to Section 5.13.4 for additional system integrity requirements related to mobile devices used to access CJI.

5.10.1 Information Flow Enforcement

The network infrastructure shall control the flow of information between interconnected systems. Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. In other words, controlling how data moves from one place to the next in a secure manner. Examples of controls that are better expressed as flow control than access control (see Section 5.5) are:

1. Prevent CJI from being transmitted unencrypted across the public network.
2. Block outside traffic that claims to be from within the agency.
3. Do not pass any web requests to the public network that are not from the internal web proxy.

Specific examples of flow control enforcement can be found in boundary protection devices (e.g. proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict information system services or provide a packet filtering capability.

5.10.1.1 Boundary Protection

The agency shall:

1. Control access to networks processing CJI.
2. Monitor and control communications at the external boundary of the information system and at key internal boundaries within the system.
3. Ensure any connections to the Internet, other external networks, or information systems occur through controlled interfaces (e.g. proxies, gateways, routers, firewalls, encrypted tunnels). See Section 5.13.4.4 for guidance on personal firewalls.
4. Employ tools and techniques to monitor network events, detect attacks, and provide identification of unauthorized use.
5. Ensure the operational failure of the boundary protection mechanisms do not result in any unauthorized release of information outside of the information system boundary (i.e. the device shall "fail closed" vs. "fail open").

6. Allocate publicly accessible information system components (e.g. public Web servers) to separate sub networks with separate, network interfaces. Publicly accessible information systems residing on a virtual host shall follow the guidance in Section 5.10.3.2 to achieve separation.

5.10.1.2 Encryption

Commonly available encryption tools often use a key to unlock the cipher to allow data access; this key is called a passphrase. While similar to a password, a passphrase is not used for user authentication. Additionally, the passphrase contains stringent character requirements making it more secure and thus providing a higher level of confidence that the passphrase will not be compromised.

1. Encryption shall be a minimum of 128 bit.
2. When CJI is transmitted outside the boundary of the physically secure location, the data shall be immediately protected via cryptographic mechanisms (encryption).

EXCEPTIONS: See Sections 5.5.7.3.2 and 5.10.2.

3. When CJI is at rest (i.e. stored electronically) outside the boundary of the physically secure location, the data shall be protected via cryptographic mechanisms (encryption).
 - a) When agencies implement encryption on CJI at rest, the passphrase used to unlock the cipher shall meet the following requirements:
 - i. Be at least 10 characters
 - ii. Not be a dictionary word.
 - iii. Include at least one (1) upper case letter, one (1) lower case letter, one (1) number, and one (1) special character.
 - iv. Be changed when previously authorized personnel no longer require access.
 - b) Multiple files maintained in the same unencrypted folder shall have separate and distinct passphrases. A single passphrase may be used to encrypt an entire folder or disk containing multiple files. All audit requirements found in Section 5.4.1 Auditable Events and Content (Information Systems) shall be applied.
4. When encryption is employed, the cryptographic module used shall be certified to meet FIPS 140-2 standards.

Note 1: Subsequent versions of approved cryptographic modules that are under current review for FIPS 140-2 compliancy can be used in the interim until certification is complete.

Note 2: While FIPS 197 (Advanced Encryption Standard) certification is desirable, a FIPS 197 certification alone is insufficient as the certification is for the algorithm only vs. the FIPS 140-2 standard which certifies the packaging of an implementation.

EXCEPTION: When encryption is used for CJI at rest, agencies may use encryption methods that are FIPS 197 certified, 256 bit as described on the National Security Agency (NSA) Suite B Cryptography list of approved algorithms.

5. For agencies using public key infrastructure technology, the agency shall develop and implement a certificate policy and certification practice statement for the issuance of public key certificates used in the information system. Registration to receive a public key certificate shall:
 - a) Include authorization by a supervisor or a responsible official.
 - b) Be accomplished by a secure process that verifies the identity of the certificate holder.
 - c) Ensure the certificate is issued to the intended party.

5.10.1.3 Intrusion Detection Tools and Techniques

The agency shall implement network-based and/or host-based intrusion detection tools.

The CSA/SIB shall, in addition:

1. Monitor inbound and outbound communications for unusual or unauthorized activities.
2. Send individual intrusion detection logs to a central logging facility where correlation and analysis will be accomplished as a system wide intrusion detection effort.
3. Employ automated tools to support near-real-time analysis of events in support of detecting system-level attacks.

5.10.1.4 Voice over Internet Protocol

Voice over Internet Protocol (VoIP) has been embraced by organizations globally as an addition to, or replacement for, public switched telephone network (PSTN) and private branch exchange (PBX) telephone systems. The immediate benefits are lower costs than traditional telephone services and VoIP can be installed in-line with an organization's existing Internet Protocol (IP) services. Among VoIP's risks that have to be considered carefully are: myriad security concerns, cost issues associated with new networking hardware requirements, and overarching quality of service (QoS) factors.

In addition to the security controls described in this document, the following additional controls shall be implemented when an agency deploys VoIP within a network that contains unencrypted CJI:

1. Establish usage restrictions and implementation guidance for VoIP technologies.
2. Change the default administrative password on the IP phones and VoIP switches.
3. Utilize Virtual Local Area Network (VLAN) technology to segment VoIP traffic from data traffic.

Appendix G.2 outlines threats, vulnerabilities, mitigations, and NIST best practices for VoIP.

5.10.1.5 Cloud Computing

Organizations transitioning to a cloud environment are presented unique opportunities and challenges (e.g., purported cost savings and increased efficiencies versus a loss of control over the data). Reviewing the cloud computing white paper (Appendix G.3), the cloud assessment located within the security policy resource center on FBI.gov, NIST Special Publications (800-144, 800-145, and 800-146), as well as the cloud provider's policies and capabilities will enable organizations to make informed decisions on whether or not the cloud provider can offer service that maintains compliance with the requirements of the CJIS Security Policy.

The metadata derived from CJI shall not be used by any cloud service provider for any purposes. The cloud service provider shall be prohibited from scanning any email or data files for the purpose of building analytics, data mining, advertising, or improving the services provided.

5.10.2 Facsimile Transmission of CJI

CJI transmitted via facsimile is exempt from encryption requirements.

5.10.3 Partitioning and Virtualization

As resources grow scarce, agencies are increasing the centralization of applications, services, and system administration. Advanced software now provides the ability to create virtual machines that allows agencies to reduce the amount of hardware needed. Although the concepts of partitioning and virtualization have existed for a while, the need for securing the partitions and virtualized machines has evolved due to the increasing amount of distributed processing and federated information sources now available across the Internet.

5.10.3.1 Partitioning

The application, service, or information system shall separate user functionality (including user interface services) from information system management functionality.

The application, service, or information system shall physically or logically separate user interface services (e.g. public web pages) from information storage and management services (e.g. database management). Separation may be accomplished through the use of one or more of the following:

1. Different computers.
2. Different central processing units.
3. Different instances of the operating system.
4. Different network addresses.
5. Other methods approved by the FBI CJIS ISO.

5.10.3.2 Virtualization

Virtualization refers to a methodology of dividing the resources of a computer (hardware and software) into multiple execution environments. Virtualized environments are authorized for criminal justice and noncriminal justice activities. In addition to the security controls described in this Policy, the following additional controls shall be implemented in a virtual environment:

1. Isolate the host from the virtual machine. In other words, virtual machine users cannot access host files, firmware, etc.
2. Maintain audit logs for all virtual machines and hosts and store the logs outside the hosts' virtual environment.
3. Virtual Machines that are Internet facing (web servers, portal servers, etc.) shall be physically separate from Virtual Machines that process CJI internally.
4. Device drivers that are "critical" shall be contained within a separate guest.

The following are additional technical security control best practices and should be implemented wherever feasible:

1. Encrypt network traffic between the virtual machine and host.
2. Implement IDS and IPS monitoring within the virtual machine environment.
3. Virtually firewall each virtual machine from each other (or physically firewall each virtual machine from each other with an application layer firewall) and ensure that only allowed protocols will transact.
4. Segregate the administrative duties for the host.

Appendix G-1 provides some reference and additional background information on virtualization.

5.10.4 System and Information Integrity Policy and Procedures

5.10.4.1 Patch Management

The agency shall identify applications, services, and information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws.

The agency (or the software developer/vendor in the case of software developed and maintained by a vendor/contractor) shall develop and implement a local policy that ensures prompt installation of newly released security relevant patches, service packs and hot fixes. Local policies should include such items as:

1. Testing of appropriate patches before installation.
2. Rollback capabilities when installing patches, updates, etc.
3. Automatic updates without individual user intervention.
4. Centralized patch management.

Patch requirements discovered during security assessments, continuous monitoring or incident response activities shall also be addressed expeditiously.

5.10.4.2 Malicious Code Protection

The agency shall implement malicious code protection that includes automatic updates for all systems with Internet access. Agencies with systems not connected to the Internet shall implement local procedures to ensure malicious code protection is kept current (i.e. most recent update available).

The agency shall employ virus protection mechanisms to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses) at critical points throughout the network and on all workstations, servers and mobile computing devices on the network. The agency shall ensure malicious code protection is enabled on all of the aforementioned critical points and information systems and resident scanning is employed.

5.10.4.3 Spam and Spyware Protection

The agency shall implement spam and spyware protection.

The agency shall:

1. Employ spam protection mechanisms at critical information system entry points (e.g. firewalls, electronic mail servers, remote-access servers).
2. Employ spyware protection at workstations, servers and mobile computing devices on the network.
3. Use the spam and spyware protection mechanisms to detect and take appropriate action on unsolicited messages and spyware/adware, respectively, transported by electronic mail, electronic mail attachments, Internet accesses, removable media (e.g. diskettes or compact disks) or other removable media as defined in this Policy.

5.10.4.4 Security Alerts and Advisories

The agency shall:

1. Receive information system security alerts/advisories on a regular basis.
2. Issue alerts/advisories to appropriate personnel.
3. Document the types of actions to be taken in response to security alerts/advisories.
4. Take appropriate actions in response.
5. Employ automated mechanisms to make security alert and advisory information available throughout the agency as appropriate.

5.10.4.5 Information Input Restrictions

The agency shall restrict the information input to any connection to FBI CJIS services to authorized personnel only.

Restrictions on personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities.

5.10.5 References/Citations/Directives

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

Figure 14 – A Local Police Department's Information Systems & Communications Protections

A local police department implemented a replacement CAD system within a physically secure location that was authorized to process CJI using a FIPS 140-2 encrypted VPN tunnel over the Internet to the state's CSA. In addition to the policies, physical and personnel controls already in place, the police department employed firewalls both at their border and at key points within their network, intrusion detection systems, a patch-management strategy that included automatic patch updates where possible, virus scanners, spam and spyware detection mechanisms that update signatures automatically, and subscribed to various security alert mailing lists and addressed vulnerabilities raised through the alerts as needed.

5.11 Policy Area 11: Formal Audits

Formal audits are conducted to ensure compliance with applicable statutes, regulations and policies.

5.11.1 Audits by the FBI CJIS Division

5.11.1.1 Triennial Compliance Audits by the FBI CJIS Division

The FBI CJIS Division is authorized to conduct audits, once every three (3) years as a minimum, to assess agency compliance with applicable statutes, regulations and policies. The CJIS Audit Unit (CAU) shall conduct a triennial audit of each CSA in order to verify compliance with applicable statutes, regulations and policies. This audit shall include a sample of CJAs and, in coordination with the SIB, the NCJAs. Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with applicable statutes, regulations and policies. The FBI CJIS Division shall also have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

5.11.1.2 Triennial Security Audits by the FBI CJIS Division

The FBI CJIS Division is authorized to conduct security audits of the CSA and SIB networks and systems, once every three (3) years as a minimum, to assess agency compliance with the CJIS Security Policy. This audit shall include a sample of CJAs and NCJAs. Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with the CJIS Security Policy.

5.11.2 Audits by the CSA

Each CSA shall:

1. At a minimum, triennially audit all CJAs and NCJAs which have direct access to the state system in order to ensure compliance with applicable statutes, regulations and policies.
2. In coordination with the SIB, establish a process to periodically audit all NCJAs, with access to CJI, in order to ensure compliance with applicable statutes, regulations and policies.
3. Have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

5.11.3 Special Security Inquiries and Audits

All agencies having access to CJI shall permit an inspection team to conduct an appropriate inquiry and audit of any alleged security violations. The inspection team shall be appointed by the APB and shall include at least one representative of the CJIS Division. All results of the inquiry and audit shall be reported to the APB with appropriate recommendations.

5.11.4 References/Citations/Directives

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

Figure 15 – The Audit of a Local Police Department

A local police department implemented a replacement CAD system that integrated to their state's CSA and was authorized to process CJI. Shortly after the implementation, their state's CSA conducted an audit of their policies, procedures, and systems that process CJI. The police department supplied all architectural and policy documentation, including detailed network diagrams, to the auditors in order to assist them in the evaluation. The auditors discovered a deficiency in the police department's systems and marked them "out" in this aspect of the FBI CJIS Security Policy. The police department quickly addressed the deficiency and took corrective action, notifying the auditors of their actions.

5.12 Policy Area 12: Personnel Security

Having proper security measures against the insider threat is a critical component for the CJIS Security Policy. This section's security terms and requirements apply to all personnel who have access to unencrypted CJI including those individuals with only physical or logical access to devices that store, process or transmit unencrypted CJI.

5.12.1 Personnel Security Policy and Procedures

5.12.1.1 Minimum Screening Requirements for Individuals Requiring Access to CJI:

1. To verify identification, a state of residency and national fingerprint-based record checks shall be conducted within 30 days of assignment for all personnel who have direct access to CJI and those who have direct responsibility to configure and maintain computer systems and networks with direct access to CJI. However, if the person resides in a different state than that of the assigned agency, the agency shall conduct state (of the agency) and national fingerprint-based record checks and execute a NLETS CHRI IQ/FQ/AQ query using purpose code C, E, or J depending on the circumstances. When appropriate, the screening shall be consistent with:

(i) 5 CFR 731.106; and/or

(ii) Office of Personnel Management policy, regulations, and guidance; and/or

(iii) agency policy, regulations, and guidance.

(See Appendix J for applicable guidance regarding noncriminal justice agencies performing adjudication of civil fingerprint submissions.) Federal entities bypassing state repositories in compliance with federal law may not be required to conduct a state fingerprint-based record check.

2. All requests for access shall be made as specified by the CSO. The CSO, or their designee, is authorized to approve access to CJI. All CSO designees shall be from an authorized criminal justice agency.
3. If a felony conviction of any kind exists, the hiring authority in the Interface Agency shall deny access to CJI. However, the hiring authority may ask for a review by the CSO in extenuating circumstances where the severity of the offense and the time that has passed would support a possible variance.
4. If a record of any other kind exists, access to CJI shall not be granted until the CSO or his/her designee reviews the matter to determine if access is appropriate.
5. If the person appears to be a fugitive or has an arrest history without conviction, the CSO or his/her designee shall review the matter to determine if access to CJI is appropriate.
6. If the person is employed by a NCJA, the CSO or his/her designee, and, if applicable, the appropriate board maintaining management control, shall review the matter to determine if CJI access is appropriate. This same procedure applies if this person is found to be a fugitive or has an arrest history without conviction.

7. If the person already has access to CJI and is subsequently arrested and or convicted, continued access to CJI shall be determined by the CSO. This does not implicitly grant hiring/firing authority with the CSA, only the authority to grant access to CJI.
8. If the CSO or his/her designee determines that access to CJI by the person would not be in the public interest, access shall be denied and the person's appointing authority shall be notified in writing of the access denial.
9. Support personnel, contractors, and custodial workers with access to physically secure locations or controlled areas (during CJI processing) shall be subject to a state and national fingerprint-based record check unless these individuals are escorted by authorized personnel at all times.

It is recommended individual background re-investigations be conducted every five years unless Rap Back is implemented.

5.12.1.2 Personnel Screening for Contractors and Vendors

In addition to meeting the requirements in paragraph 5.12.1.1, contractors and vendors shall meet the following requirements:

1. Prior to granting access to CJI, the CGA on whose behalf the Contractor is retained shall verify identification via a state of residency and national fingerprint-based record check. However, if the person resides in a different state than that of the assigned agency, the agency shall conduct state (of the agency) and national fingerprint-based record checks and execute a NLETS CHRI IQ/FQ/AQ query using purpose code C, E, or J depending on the circumstances.
2. If a record of any kind is found, the CGA shall be formally notified and system access shall be delayed pending review of the criminal history record information. The CGA shall in turn notify the Contractor-appointed Security Officer.
3. When identification of the applicant with a criminal history has been established by fingerprint comparison, the CGA or the CJA (if the CGA does not have the authority to view CHRI) shall review the matter.
4. A Contractor employee found to have a criminal record consisting of felony conviction(s) shall be disqualified.
5. Applicants shall also be disqualified on the basis of confirmations that arrest warrants are outstanding for such applicants.
6. The CGA shall maintain a list of personnel who have been authorized access to CJI and shall, upon request, provide a current copy of the access list to the CSO.

Applicants with a record of misdemeanor offense(s) may be granted access if the CSO determines the nature or severity of the misdemeanor offense(s) do not warrant disqualification. The CGA may request the CSO to review a denial of access determination.

5.12.2 Personnel Termination

The agency, upon termination of individual employment, shall immediately terminate access to CJI.

5.12.3 Personnel Transfer

The agency shall review CJI access authorizations when personnel are reassigned or transferred to other positions within the agency and initiate appropriate actions such as closing and establishing accounts and changing system access authorizations.

5.12.4 Personnel Sanctions

The agency shall employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.

5.12.5 References/Citations/Directives

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

Figure 16 – A Local Police Department's Personnel Security Controls

A local police department implemented a replacement CAD system that integrated to their state's CSA and was authorized to process CJI. In addition to the physical and technical controls already in place, the police department implemented a variety of personnel security controls to reduce the insider threat. The police department used background screening consistent with the FBI CJIS Security Policy to vet those with unescorted access to areas in which CJI is processed, including the IT administrators employed by a contractor and all janitorial staff. The police department established sanctions against any vetted person found to be in violation of stated policies. The police department re-evaluated each person's suitability for access to CJI every five years.

5.13 Policy Area 13: Mobile Devices

This policy area describes considerations and requirements for mobile devices including smartphones and tablets. Mobile devices are not limited to a single form factor or communications medium. The requirements in this section augment those in other areas of the Policy to address the gaps introduced by using mobile devices.

The agency shall: (i) establish usage restrictions and implementation guidance for mobile devices; and (ii) authorize, monitor, control wireless access to the information system. Wireless technologies, in the simplest sense, enable one or more devices to communicate without physical connections—without requiring network or peripheral cabling.

Appendix G provides reference material and additional information on mobile devices.

5.13.1 Wireless Communications Technologies

Examples of wireless communication technologies include, but are not limited to: 802.11x, cellular, Bluetooth, satellite, microwave, and land mobile radio (LMR). Wireless technologies require at least the minimum security applied to wired technology and, based upon the specific technology or implementation, wireless technologies may require additional security controls as described below.

5.13.1.1 All 802.11 Wireless Protocols

Agencies shall implement the following controls for all agency-managed wireless access points:

1. Perform validation testing to ensure rogue APs (Access Points) do not exist in the 802.11 Wireless Local Area Network (WLAN) and to fully understand the wireless network security posture.
2. Maintain a complete inventory of all Access Points (APs) and 802.11 wireless devices.
3. Place APs in secured areas to prevent unauthorized physical access and user manipulation.
4. Test AP range boundaries to determine the precise extent of the wireless coverage and design the AP wireless coverage to limit the coverage area to only what is needed for operational purposes.
5. Enable user authentication and encryption mechanisms for the management interface of the AP.
6. Ensure that all APs have strong administrative passwords and ensure that all passwords are changed in accordance with Section 5.6.2.1.
7. Ensure the reset function on APs is used only when needed and is only invoked by authorized personnel. Restore the APs to the latest security settings, when the reset functions are used, to ensure the factory default settings are not utilized.
8. Change the default service set identifier (SSID) in the APs. Disable the broadcast SSID feature so that the client SSID must match that of the AP. Validate that the SSID character string does not contain any agency identifiable information (division, department, street, etc.) or services.

9. Enable all security features of the wireless product, including the cryptographic authentication, firewall, and other available privacy features.
10. Ensure that encryption key sizes are at least 128-bits and the default shared keys are replaced by unique keys.
11. Ensure that the ad hoc mode has been disabled.
12. Disable all nonessential management protocols on the APs and disable hypertext transfer protocol (HTTP) when not needed or protect HTTP access with authentication and encryption.
13. Enable logging (if supported) and review the logs on a recurring basis per local policy. At a minimum logs shall be reviewed monthly.
14. Insulate, virtually (e.g. virtual local area network (VLAN) and ACLs) or physically (e.g. firewalls), the wireless network from the operational wired infrastructure. Limit access between wireless networks and the wired network to only operational needs.
15. When disposing of access points that will no longer be used by the agency, clear access point configuration to prevent disclosure of network configuration, keys, passwords, etc.

5.13.1.2 Cellular

Cellular telephones, smartphones (i.e. Blackberry, iPhones, etc.), tablets, personal digital assistants (PDA), and “aircards” are examples of cellular handheld devices or devices that are capable of employing cellular technology. Additionally, cellular handheld devices typically include Bluetooth, infrared, and other wireless protocols capable of joining infrastructure networks or creating dynamic ad hoc networks.

Threats to cellular handheld devices stem mainly from their size, portability, and available wireless interfaces and associated services. Examples of threats to cellular handheld devices include:

1. Loss, theft, or disposal.
2. Unauthorized access.
3. Malware.
4. Spam.
5. Electronic eavesdropping.
6. Electronic tracking (threat to security of data and safety of law enforcement officer).
7. Cloning (not as prevalent with later generation cellular technologies).
8. Server-resident data.

5.13.1.2.1 Cellular Service Abroad

Certain internal functions on cellular devices may be modified or compromised by the cellular carrier during international use as the devices are intended to have certain parameters configured by the cellular provider which is considered a “trusted” entity by the device.

When devices are authorized for use outside the U.S., agencies shall perform an inspection to ensure that all controls are in place and functioning properly in accordance with the agency's policies.

5.13.1.2.2 Voice Transmissions Over Cellular Devices

Any cellular device used to transmit CJI via voice is exempt from the encryption and authentication requirements.

5.13.1.3 Bluetooth

Bluetooth is an open standard for short-range radio frequency (RF) communication. Bluetooth is used primarily to establish wireless personal area networks (WPAN). Bluetooth technology has been integrated into many types of business and consumer devices, including cell phones, laptops, automobiles, medical devices, printers, keyboards, mice, headsets, and biometric capture devices.

Bluetooth technology and associated devices are susceptible to general wireless networking threats (e.g. denial of service [DoS] attacks, eavesdropping, man-in-the-middle [MITM] attacks, message modification, and resource misappropriation) as well as specific Bluetooth-related attacks that target known vulnerabilities in Bluetooth implementations and specifications. Organizational security policy shall be used to dictate the use of Bluetooth and its associated devices based on the agency's operational and business processes.

5.13.2 Mobile Device Management (MDM)

Mobile Device Management (MDM) facilitates the implementation of sound security controls for mobile devices and allows for centralized oversight of configuration control, application usage, and device protection and recovery, if so desired by the agency.

Due to the potential for inconsistent network access or monitoring capability on mobile devices, methods used to monitor and manage the configuration of full featured operating systems may not function properly on devices with limited feature operating systems. MDM systems and applications coupled with device specific technical policy can provide a robust method for device configuration management if properly implemented.

Devices that have had any unauthorized changes made to them (including but not limited to being rooted or jailbroken) shall not be used to process, store, or transmit CJI data at any time. Agencies shall implement the following controls when allowing CJI access from cell/smartphones and tablet devices:

1. Ensure that CJI is only transferred between CJI authorized applications and storage areas of the device.
2. MDM with centralized administration configured and implemented to perform at least the:
 - i. Remote locking of device
 - ii. Remote wiping of device
 - iii. Setting and locking device configuration
 - iv. Detection of "rooted" and "jailbroken" devices
 - v. Enforcement of folder or disk level encryption
 - vi. Application of mandatory policy settings on the device

- vii. Detection of unauthorized configurations or software/applications

5.13.3 Wireless Device Risk Mitigations

Organizations shall, at a minimum, ensure that cellular wireless devices:

1. Apply available critical patches and upgrades to the operating system as soon as they become available for the device and after necessary testing as described in Section 5.10.4.1.
2. Are configured for local device authentication (see Section 5.13.9.1).
3. Use advanced authentication.
4. Encrypt all CJI resident on the device.
5. Erase cached information, to include authenticators (see Section 5.6.2.1) in applications, when session is terminated.
6. Employ personal firewalls or run a Mobile Device Management (MDM) system that facilitates the ability to provide firewall services from the agency level.
7. Employ antivirus software or run a MDM system that facilitates the ability to provide antivirus services from the agency level.

5.13.3.1 Legacy 802.11 Protocols

Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) cryptographic algorithms, used by all pre-802.11i protocols, do not meet the requirements for FIPS 140-2 and shall not be used.

5.13.4 System Integrity

Managing system integrity on limited function mobile operating systems may require methods and technologies significantly different from traditional full featured operating systems. In many cases, the requirements of Section 5.10 of the CJIS Security Policy cannot be met with a mobile device without the installation of a third party MDM, application, or supporting service infrastructure.

5.13.4.1 Patching/Updates

Based on the varying connection methods for mobile devices, an always on connection cannot be guaranteed for patching and updating. Devices without always-on cellular connections may not be reachable for extended periods of time by the MDM or solution either to report status or initiate patching.

Agencies shall monitor mobile devices not capable of an always-on cellular connection (i.e. WiFi only or WiFi with cellular on demand) to ensure their patch and update state is current.

5.13.4.2 Malicious Code Protection

Appropriately configured MDM software is capable of checking the installed applications on the device and reporting the software inventory to a central management console in a manner analogous to traditional virus scan detection of unauthorized software and can provide a high degree of confidence that only known software or applications are installed on the device.

Agencies that allow smartphones and tablets to access CJI shall have a process to approve the use of specific software or applications on the devices. An appropriately configured MDM shall be used on smartphones and tablets to prevent the installation of unauthorized software or applications.

5.13.4.3 Physical Protection

Due to small form factors and the fact that mobile devices are often stored in lower security areas, the risk to theft or loss of the device and any data stored on it is elevated. Physical protections will often be the responsibility of the assigned device user.

When mobile devices are authorized for use to access CJI are lost or stolen, agencies shall:

1. Have the ability to determine the location of agency controlled smartphones and tablets.
2. Immediately wipe the device.

5.13.4.4 Personal Firewall

For the purpose of this policy, a personal firewall is an application that controls network traffic to and from a user device, permitting or denying communications based on policy. A personal firewall shall be employed on all mobile devices that have a full-feature operating system (i.e. laptops or tablets with Windows or Linux/Unix operating systems). At a minimum, the personal firewall shall perform the following activities:

1. Manage program access to the Internet.
2. Block unsolicited requests to connect to the user device.
3. Filter incoming traffic by IP address or protocol.
4. Filter incoming traffic by destination ports.
5. Maintain an IP traffic log.

Mobile devices with limited feature operating systems (i.e. tablets, smartphones) may not support a personal firewall. However, these operating systems have a limited number of system services installed, carefully controlled network access, and to a certain extent, perform similar functions a personal firewall would provide on a device with a full feature operating system. Appropriately configured MDM software is capable of controlling which applications are allowed on the device.

5.13.5 Incident Response

In addition to the requirements in Section 5.3 Incident Response, agencies shall develop additional or enhanced incident reporting and handling procedures to address mobile device operating scenarios. Rapid response to mobile device related incidents can significantly mitigate the risks associated with illicit data access either on the device itself or within online data resources associated with the device through an application or specialized interface.

Special reporting procedures for mobile devices shall apply in any of the following situations:

1. Loss of device control
 - a. Device known to be locked, minimal duration of loss
 - b. Device lock state unknown, minimal duration of loss
 - c. Device lock state unknown, extended duration of loss
 - d. Device known to be unlocked, more than momentary duration of loss
2. Total loss of device
 - a. CJI stored on device
 - b. Lock state of device
 - c. Capabilities for remote tracking or wiping of device
3. Device compromise
4. Device loss or compromise outside the United States

5.13.6 Auditing and Accountability

The ability to implement audit and accountability functions may not be natively included on mobile devices with limited function operating systems (e.g. Android, Apple iOS). Either additional device management systems or auditing from systems accessed by the mobile device may be necessary to ensure appropriate levels of auditing exist. Additionally, the type of connectivity capable by the device will also affect the ability to collect audit logs for review.

A mobile device not capable of providing required audit and accountability on its own accord shall be monitored by a MDM, other management system, or application capable of collecting required log data.

5.13.7 Access Control

Multiple user accounts are not generally supported on limited function mobile operating systems. This may mean the policy requirements for access control (Section 5.5 Access Control, regarding account management) would not apply to the operating system, but rather to a particular application, either stand-alone to the device or as part of a client server architecture.

5.13.8 Wireless Hotspot Capability

Many mobile devices include the capability to function as a wireless access point or WiFi hotspot that allows other devices to connect through the device to the internet over the devices cellular network.

When an agency allows mobile devices to function as a wireless access point, they shall be configured:

1. In accordance with the requirements in section 5.13.1.1 All 802.11 Wireless Protocols
2. To only allow connections from agency authorized devices

5.13.9 Identification and Authentication

Due to the technical methods used for identification and authentication on many limited feature mobile operating systems, achieving compliance may require many different components.

5.13.9.1 Local Device Authentication

When mobile devices are authorized for use in accessing CJI, local device authentication shall be used to unlock the device for use. The authenticator used shall meet the requirements in section 5.6.2.1 Standard Authenticators.

5.13.10 Device Certificates

Device certificates are often used to uniquely identify mobile devices using part of a public key pair on the device in the form of a public key certificate. While there is value to ensuring the device itself can authenticate to a system supplying CJI, and may provide a critical layer of device identification or authentication in a larger scheme, a device certificate alone placed on the device shall not be considered valid proof that the device is being operated by an authorized user.

When certificates or cryptographic keys used to authenticate a mobile device are stored on the device, they shall be:

1. Protected against being extracted from the device
2. Configured for remote wipe on demand or self-deletion based on a number of unsuccessful login or access attempts
3. Configured to use a secure authenticator (i.e. password, PIN) to unlock the key for use

APPENDICES

APPENDIX A TERMS AND DEFINITIONS

Access to Criminal Justice Information — The physical or logical (electronic) ability, right or privilege to view, modify or make use of Criminal Justice Information.

Administration of Criminal Justice — The detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. It also includes criminal identification activities; the collection, storage, and dissemination of criminal history record information; and criminal justice employment. In addition, administration of criminal justice includes “crime prevention programs” to the extent access to criminal history record information is limited to law enforcement agencies for law enforcement programs (e.g. record checks of individuals who participate in Neighborhood Watch or “safe house” programs) and the result of such checks will not be disseminated outside the law enforcement agency.

Agency Controlled Mobile Device — A mobile device that is centrally managed by an agency for the purpose of securing the device for potential access to CJI. The device can be agency issued or BYOD (personally owned).

Agency Coordinator (AC) — A staff member of the Contracting Government Agency who manages the agreement between the Contractor and agency.

Agency Issued Mobile Device — A mobile device that is owned by an agency and issued to an individual for use. It is centrally managed by the agency for the purpose of securing the device for potential access to CJI. The device is not BYOD (personally owned).

Agency Liaison (AL) — Coordinator of activities between the criminal justice agency and the noncriminal justice agency when responsibility for a criminal justice system has been delegated by a criminal justice agency to a noncriminal justice agency, which has in turn entered into an agreement with a contractor. The agency liaison shall, inter alia, monitor compliance with system security requirements. In instances in which the noncriminal justice agency's authority is directly from the CJIS systems agency, there is no requirement for the appointment of an agency liaison.

Authorized User/Personnel — An individual, or group of individuals, who have been appropriately vetted through a national fingerprint-based record check and have been granted access to CJI.

Authorized Recipient — (1) A criminal justice agency or federal agency authorized to receive CHRI pursuant to federal statute or executive order; (2) A nongovernmental entity authorized by federal statute or executive order to receive CHRI for noncriminal justice purposes; or (3) A government agency authorized by federal statute or executive order, or state statute which has been approved by the United States Attorney General to receive CHRI for noncriminal justice purposes.

Availability — The degree to which information, a system, subsystem, or equipment is operable and in a useable state; frequently represented as a proportion of time the element is in a functioning condition.

Biographic Data — Information collected about individuals associated with a unique case, and not necessarily connected to identity data. Biographic Data does not provide a history of an individual, only information related to a unique case.

Biometric Data — When applied to CJI, it is used to identify individuals, and includes the following types: finger prints, palm prints, DNA, iris, and facial recognition.

Case / Incident History — All relevant information gathered about an individual, organization, incident, or combination thereof, arranged so as to serve as an organized record to provide analytic value for a criminal justice organization. In regards to CJI, it is the information about the history of criminal incidents.

Channeler — An FBI approved contractor, who has entered into an agreement with an Authorized Recipient(s), to receive noncriminal justice applicant fingerprint submissions and collect the associated fees. The Channeler ensures fingerprint submissions are properly and adequately completed, electronically forwards fingerprint submissions to the FBI's CJIS Division for national noncriminal justice criminal history record check, and receives electronic record check results for dissemination to Authorized Recipients. A Channeler is essentially an "expediter" rather than a user of criminal history record check results.

Cloud Client – A machine or software application that accesses cloud services over a network connection, perhaps on behalf of a subscriber.

Cloud Computing – A distributed computing model that permits on-demand network access to a shared pool of configurable computing resources (i.e., networks, servers, storage, applications, and services), software, and information.

Cloud Provider – An organization that provides cloud computing services.

Cloud Subscriber – A person or organization that is a customer of a cloud computing service provider.

CJIS Advisory Policy Board (APB) — The governing organization within the FBI CJIS Advisory Process composed of representatives from criminal justice and national security agencies within the United States. The APB reviews policy, technical, and operational issues relative to CJIS Division programs and makes subsequent recommendations to the Director of the FBI.

CJIS Audit Unit (CAU) — The organization within the FBI CJIS Division responsible to perform audits of CSAs to verify compliance with the CJIS Security Policy.

CJIS Security Policy — The FBI CJIS Security Policy document as published by the FBI CJIS ISO; the document containing this glossary.

CJIS Systems Agency (CSA) — A duly authorized state, federal, international, tribal, or territorial criminal justice agency on the CJIS network providing statewide (or equivalent) service to its criminal justice users with respect to the CJI from various systems managed by the FBI CJIS Division. There shall be only one CSA per state or territory. In federal agencies, the CSA may be the interface or switch to other federal agencies connecting to the FBI CJIS systems.

CJIS Systems Agency Information Security Officer (CSA ISO) — The appointed FBI CJIS Division personnel responsible to coordinate information security efforts at all CJIS interface agencies.

CJIS Systems Officer (CSO) — An individual located within the CJIS Systems Agency responsible for the administration of the CJIS network on behalf for the CJIS Systems Agency.

Compact Council — The entity created by the National Crime Prevention and Privacy Compact of 1998 that has the authority to promulgate rules and procedures governing the use of the III system for noncriminal justice purposes.

Compact Officers — The leadership of the Compact Council, oversees the infrastructure established by the National Crime Prevention and Privacy Compact Act of 1998, which is used by ratifying states to exchange criminal records for noncriminal justice purposes. Their primary responsibilities are to promulgate rules and procedures for the effective and appropriate use of the III system.

Compensating Controls – Compensating controls are temporary control measures implemented in lieu of the required control measures when an agency cannot meet the AA requirement due to legitimate technical or business constraints. The compensating controls must:

1. Meet the intent of the CJIS Security Policy AA requirement
2. Provide a similar level of protection or security as the original AA requirement
3. Not rely upon the existing requirements for AA as compensating controls

Additionally, compensating controls may rely upon other, non-AA, existing requirements as compensating controls and/or be combined with new controls to create compensating controls.

Computer Security Incident Response Capability (CSIRC) — A collection of personnel, systems, and processes that are used to efficiently and quickly manage a centralized response to any sort of computer security incident which may occur.

Confidentiality — The concept of ensuring that information is observable only to those who have been granted authorization to do so.

Contractor — A private business, agency or individual which has entered into an agreement for the administration of criminal justice or noncriminal justice functions with a Criminal Justice Agency or a Noncriminal Justice Agency. Also, a private business approved by the FBI CJIS Division to contract with Noncriminal Justice Agencies to perform noncriminal justice functions associated with civil fingerprint submission for hiring purposes.

Contracting Government Agency (CGA) — The government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor.

Crime Reports Data — The data collected through the Uniform Crime Reporting program and reported upon annually by the FBI CJIS division used to analyze the crime statistics for the United States.

Criminal History Record Information (CHRI) — A subset of CJL. Any notations or other written or electronic evidence of an arrest, detention, complaint, indictment, information or other

formal criminal charge relating to an identifiable person that includes identifying information regarding the individual as well as the disposition of any charges.

Criminal Justice Agency (CJA) — The courts, a governmental agency, or any subunit of a governmental agency which performs the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice. State and federal Inspectors General Offices are included.

Criminal Justice Agency User Agreement — A terms-of-service agreement that must be signed prior to accessing CJI. This agreement is required by each CJA and spells out user's responsibilities, the forms and methods of acceptable use, penalties for their violation, disclaimers, and so on.

Criminal Justice Conveyance — A criminal justice conveyance is any mobile vehicle used for the purposes of criminal justice activities with the capability to comply, during operational periods, with the requirements of Section 5.9.1.3.

Criminal Justice Information (CJI) — Criminal Justice Information is the abstract term used to refer to all of the FBI CJIS provided data necessary for law enforcement agencies to perform their mission and enforce the laws, including but not limited to: biometric, identity history, person, organization, property (when accompanied by any personally identifiable information), and case/incident history data. In addition, CJI refers to the FBI CJIS-provided data necessary for civil agencies to perform their mission; including, but not limited to data used to make hiring decisions. The following type of data are exempt from the protection levels required for CJI: transaction control type numbers (e.g. ORI, NIC, FNU, etc.) when not accompanied by information that reveals CJI or PII.

Criminal Justice Information Services Division (FBI CJIS or CJIS) — The FBI division responsible for the collection, warehousing, and timely dissemination of relevant CJI to the FBI and to qualified law enforcement, criminal justice, civilian, academic, employment, and licensing agencies.

Data — See Information and CJI.

Degauss — Neutralize a magnetic field to erase information from a magnetic disk or other storage device. In the field of information technology, degauss has become synonymous with erasing information whether or not the medium is magnetic. In the event the device to be degaussed is not magnetic (e.g. solid state drive, USB storage device), steps other than magnetic degaussing may be required to render the information irretrievable from the device.

Department of Justice (DoJ) — The Department within the U.S. Government responsible to enforce the law and defend the interests of the United States according to the law, to ensure public safety against threats foreign and domestic, to provide federal leadership in preventing and controlling crime, to seek just punishment for those guilty of unlawful behavior, and to ensure fair and impartial administration of justice for all Americans.

Digital Media – Any form of electronic media designed to store data in a digital format. This includes, but is not limited to: memory device in laptops, computers, and mobile devices; and any removable, transportable electronic media, such as mandated tape or disk, optical disk, flash drives, external hard drives, or digital memory card.

Digital Signature – A digital signature consists of three algorithms: (1) A key generation algorithm that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key. (2) A signing algorithm that, given a message and a private key, produces a signature. (3) A signature verifying algorithm that, given a message, public key, and a signature, either accepts or rejects the message's claim to authenticity. Two main properties are required. First, a signature generated from a fixed message and fixed private key should verify the authenticity of that message by using the corresponding public key. Secondly, it should be computationally infeasible to generate a valid signature for a party who does not possess the private key.

Direct Access — (1) Having the authority to access systems managed by the FBI CJIS Division, whether by manual or automated methods, not requiring the assistance of, or intervention by, any other party or agency (28 CFR, Chapter 1, Part 20). (2) Having the authority to query or update national databases maintained by the FBI CJIS Division including national queries and updates automatically or manually generated by the CSA.

Dissemination — The transmission/distribution of CJI to Authorized Recipients within an agency.

Escort – Authorized personnel who accompany a visitor at all times while within a physically secure location to ensure the protection and integrity of the physically secure location and any Criminal Justice Information therein. The use of cameras or other electronic means used to monitor a physically secure location does not constitute an escort.

Federal Bureau of Investigation (FBI) — The agency within the DOJ responsible to protect and defend the United States against terrorist and foreign intelligence threats, to uphold and enforce the criminal laws of the United States, and to provide leadership and criminal justice services to federal, state, municipal, and international agencies and partners.

FBI CJIS Information Security Officer (FBI CJIS ISO) — The FBI personnel responsible for the maintenance and dissemination of the FBI CJIS Security Policy; the liaison between the FBI and the CSA's ISOs and other relevant security points-of-contact (POCs); the provider of technical guidance as to the intent and implementation of technical policy issues; the POC for computer incident notification which also disseminates security alerts to the CSOs and ISOs.

Federal Information Security Management Act (FISMA) — The Federal Information Security Management Act of 2002, a US Federal law that established information security standards for the protection of economic and national security interests of the United States. It requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

For Official Use Only (FOUO) — A caveat applied to unclassified sensitive information that may be exempt from mandatory release to the public under the Freedom of Information Act (FOIA), 5 U.S.C 522. In general, information marked FOUO shall not be disclosed to anybody except Government (Federal, State, tribal, or local) employees or contractors with a need to know.

Guest Operating System — An operating system that has emulated hardware presented to it by a host operating system. Also referred to as the virtualized operating system.

Host Operating System — In the context of virtualization, the operating system that interfaces with the actual hardware and arbitrates between it and the guest operating systems. It is also referred to as a hypervisor.

Hypervisor — See Host Operating System.

Identity History Data — Textual data that corresponds with an individual's biometric data, providing a history of criminal and/or civil events for the identified individual.

Indirect Access – Having the authority to access systems containing CJI without providing the user the ability to conduct transactional activities (the capability to query or update) on state and national systems (e.g. CJIS Systems Agency (CSA), State Identification Bureau (SIB), or national repositories).

Information — See data and CJI.

Information Exchange Agreement — An agreement that codifies the rules by which two parties engage in the sharing of information. These agreements typically include language which establishes some general duty-of-care over the other party's information, whether and how it can be further disseminated, penalties for violations, the laws governing the agreement (which establishes venue), procedures for the handling of shared information at the termination of the agreement, and so on. This document will ensure consistency with applicable federal laws, directives, policies, regulations, standards and guidance.

Information Security Officer (ISO) — Typically a member of an organization who has the responsibility to establish and maintain information security policy, assesses threats and vulnerabilities, performs risk and control assessments, oversees the governance of security operations, and establishes information security training and awareness programs. The ISO also usually interfaces with security operations to manage implementation details and with auditors to verify compliance to established policies.

Information System — A system of people, data, and processes, whether manual or automated, established for the purpose of managing information.

Integrated Automated Fingerprint Identification System (IAFIS) — The national fingerprint and criminal history system maintained by the FBI CJIS Division that provides the law enforcement community with automated fingerprint search capabilities, latent searching capability, electronic image storage, and electronic exchange of fingerprints and responses.

Integrity — The perceived consistency of expected outcomes, actions, values, and methods of an individual or organization. As it relates to data, it is the concept that data is preserved in a consistent and correct state for its intended use.

Interconnection Security Agreement (ISA) — An agreement much like an Information Exchange Agreement as mentioned above, but concentrating more on formalizing the technical and security requirements pertaining to some sort of interface between the parties' information systems.

Interface Agency — A legacy term used to describe agencies with direct connections to the CSA. This term is now used predominantly in a common way to describe any sub-agency of a CSA or SIB that leverages the CSA or SIB as a conduit to FBI CJIS information.

Internet Protocol (IP) — A protocol used for communicating data across a packet-switched internetwork using the Internet Protocol Suite, also referred to as TCP/IP. IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering distinguished protocol datagrams (packets) from the source host to the destination host solely based on their addresses.

Interstate Identification Index (III) — The CJIS service that manages automated submission and requests for CHRI that is warehoused subsequent to the submission of fingerprint information. Subsequent requests are directed to the originating State as needed.

Jailbreak (Jailbroken) — The process of attaining privileged control (known as “root access”) of a device running the Apple iOS operating system that ultimately allows a user the ability to alter or replace system applications and settings, run specialized applications that require administrator-level permissions, or perform other operations that are otherwise not allowed.

Laptop Devices – Laptop devices are mobile devices with a full-featured operating system (e.g. Microsoft Windows, Apple OS X, LINUX/UNIX, etc.). Laptops are typically intended for transport via vehicle mount or portfolio-sized carry case, but not on the body. This definition does not include pocket/handheld devices (e.g. smartphones), or mobile devices that feature a limited feature operating system (e.g. tablets).

Law Enforcement Online (LEO) — A secure, Internet-based communications portal provided by the FBI CJIS Division for use by law enforcement, first responders, criminal justice professionals, and anti-terrorism and intelligence agencies around the globe. Its primary purpose is to provide a platform on which various law enforcement agencies can collaborate on FOUO matters.

Logical Access – The technical means (e.g., read, create, modify, delete a file, execute a program, or use an external connection) for an individual or other computer system to utilize CJI or CJIS applications.

Local Agency Security Officer (LASO) — The primary Information Security contact between a local law enforcement agency and the CSA under which this agency interfaces with the FBI CJIS Division. The LASO actively represents their agency in all matters pertaining to Information Security, disseminates Information Security alerts and other material to their constituents, maintains Information Security documentation (including system configuration data), assists with Information Security audits of hardware and procedures, and keeps the CSA informed as to any Information Security needs and problems.

Management Control Agreement (MCA) — An agreement between parties that wish to share or pool resources that codifies precisely who has administrative control over, versus overall management and legal responsibility for, assets covered under the agreement. An MCA must ensure the CJA’s authority remains with regard to all aspects of Section 3.2.2. The MCA usually results in the CJA having ultimate authority over the CJI supporting infrastructure administered by the NCJA.

Mobile Device — Any portable device used to access CJI via a wireless connection (e.g. cellular, WiFi, Bluetooth, etc.).

Mobile Device Management (MDM) — Centralized administration and control of mobile devices specifically including, but not limited to, cellular phones, smart phones, and tablets. Management typically includes the ability to configure device settings and prevent a user from

changing them, remotely locating a device in the event of theft or loss, and remotely locking or wiping a device. Management can also include over-the-air distribution of applications and updating installed applications.

National Crime Information Center (NCIC) — An information system which stores CJI which can be queried by appropriate Federal, state, and local law enforcement and other criminal justice agencies.

National Instant Criminal Background Check System (NICS) — A system mandated by the Brady Handgun Violence Prevention Act of 1993 that is used by Federal Firearms Licensees (FFLs) to instantly determine via telephone or other electronic means whether the transfer of a firearm would be in violation of Section 922 (g) or (n) of Title 18, United States Code, or state law, by evaluating the prospective buyer's criminal history.

National Institute of Standards and Technology (NIST) — Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Department of Commerce whose mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic and national security.

Noncriminal Justice Agency (NCJA) — A governmental agency, or any subunit thereof, that provides services primarily for purposes other than the administration of criminal justice. Examples of services include, but not limited to, employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

NCJA (Government) — A Federal, state, local, or tribal governmental agency or any subunit thereof whose charter does not include the responsibility to administer criminal justice, but may have a need to process CJI. An example would be the central IT organization within a state government that administers equipment on behalf of a state law-enforcement agency.

NCJA (Private) — A private agency or subunit thereof whose charter does not include the responsibility to administer criminal justice, but may have a need to process CJI. An example would include a local bank.

NCJA (Public) — A public agency or sub-unit thereof whose charter does not include the responsibility to administer criminal justice, but may have a need to process CJI. An example would include a county school board which uses CHRI to assist in employee hiring decisions.

Noncriminal Justice Purpose — The uses of criminal history records for purposes authorized by federal or state law other than purposes relating to the administration of criminal justice, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

Office of Management and Budget (OMB) — The agency within the Executive Branch of the Federal government responsible to oversee the preparation of the federal budget, to assist in the supervision of other Executive Branch agencies, and to oversee and coordinate the Presidential Administration's procurement, financial management, information, and regulatory policies.

Outsourcing — The process of delegating in-house operations to a third-party. For instance, when the administration of criminal justice functions (network operations, dispatch functions, system administration operations, etc.) are performed for the criminal justice agency by a city or county information technology department or are contracted to be performed by a vendor.

Outsourcing Standard — National Crime Prevention and Privacy Compact Council's Outsourcing Standard. The Compact Council's uniform standards and processes for the interstate and Federal-State exchange of criminal history records for noncriminal justice purposes.

Personal Firewall — An application which controls network traffic to and from a computer, permitting or denying communications based on a security policy.

Personally Identifiable Information (PII) — PII is information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name.

Physical Access – The physical ability, right or privilege to view, modify or make use of Criminal Justice Information (CJI) by means of physical presence within the proximity of computers and network devices (e.g. the ability to insert a boot disk or other device into the system, make a physical connection with electronic equipment, etc.).

Physical Media – Physical media refers to media in printed form. This definition includes, but is not limited to, printed documents, printed imagery, printed facsimile.

Physically Secure Location — A facility, a police vehicle, or an area, a room, or a group of rooms, within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems.

Pocket/Handheld Mobile Device – Pocket/Handheld mobile devices (e.g. smartphones) are intended to be carried in a pocket or holster attached to the body and feature an operating system with limited functionality (e.g., iOS, Android, BlackBerry, etc.). This definition does not include tablet and laptop devices.

Property Data — Information about vehicles and property associated with a crime.

Rap Back — An IAFIS service that allows authorized agencies to receive notification of subsequent criminal activity reported to the FBI committed by persons of interest.

Receive-Only Terminal (ROT) – A device that is configured to accept a limited type of data but is technically prohibited from forming or transmitting data, browsing or navigating internal or external networks, or otherwise performing outside the scope of receive only (e.g., a printer, dumb terminal, etc.).

Repository Manager, or Chief Administrator — The designated manager of the agency having oversight responsibility for a CSA's fingerprint identification services. If both state fingerprint identification services and CJIS systems control are managed within the same state agency, the repository manager and CSO may be the same person.

Root (Rooting, Rooted) — The process of attaining privileged control (known as "root access") of a device running the Android operating system that ultimately allows a user the ability to alter or replace system applications and settings, run specialized applications that require administrator-level permissions, or perform other operations that are otherwise not allowed.

Secondary Dissemination — The promulgation of CJI from a releasing agency to an authorized recipient agency when the recipient agency has not been previously identified in a formal information exchange agreement.

Security Addendum (SA) — A uniform addendum to an agreement between the government agency and a private contractor, approved by the Attorney General of the United States, which specifically authorizes access to criminal history record information, limits the use of the information to the purposes for which it is provided, ensures the security and confidentiality of the information consistent with existing regulations and the CJIS Security Policy, provides for sanctions, and contains such other provisions as the Attorney General may require.

Sensitive But Unclassified (SBU) — Designation of information in the United States federal government that, though unclassified, often requires strict controls over its distribution. SBU is a broad category of information that includes material covered by such designations as For Official Use Only (FOUO), Law Enforcement Sensitive (LES), Sensitive Homeland Security Information, Security Sensitive Information (SSI), Critical Infrastructure Information (CII), etc. Some categories of SBU information have authority in statute or regulation (e.g. SSI, CII) while others, including FOUO, do not. As of May 9, 2008, the more appropriate terminology to use is Controlled Unclassified Information (CUI).

Service — The organized system of apparatus, appliances, personnel, etc, that supply some tangible benefit to the consumers of this service. In the context of CJI, this usually refers to one of the applications that can be used to process CJI.

Shredder — A device used for shredding documents, often as a security measure to prevent unapproved persons from reading them. Strip-cut shredders, also known as straight-cut or spaghetti-cut, slice the paper into long, thin strips but are not considered secure. Cross-cut shredders provide more security by cutting paper vertically and horizontally into confetti-like pieces.

Smartphone – See pocket/handheld mobile devices.

Social Engineering — The act of manipulating people into performing actions or divulging confidential information. While similar to a confidence trick or simple fraud, the term typically applies to trickery or deception for the purpose of information gathering, fraud, or computer system access; in most cases the attacker never comes face-to-face with the victim.

Software Patch — A piece of software designed to fix problems with, or update, a computer program or its supporting data. This includes fixing security vulnerabilities and other bugs and improving the usability or performance. Though meant to fix problems, poorly designed patches can sometimes introduce new problems. As such, patches should be installed in a test environment prior to being installed in a live, operational system. Patches often can be found in multiple locations but should be retrieved only from sources agreed upon through organizational policy.

State and Federal Agency User Agreement — A written agreement that each CSA or SIB Chief shall execute with the FBI CJIS Division stating their willingness to demonstrate conformance with the FBI CJIS Security Policy prior to the establishment of connectivity between organizations. This agreement includes the standards and sanctions governing use of CJIS systems, as well as verbiage to allow the FBI to periodically audit the CSA as well as to allow the FBI to penetration test its own network from the CSA's interfaces to it.

State Compact Officer — The representative of a state that is party to the National Crime Prevention and Privacy Compact, and is the chief administrator of the state's criminal history

record repository or a designee of the chief administrator who is a regular full-time employee of the repository.

State Identification Bureau (SIB) — The state agency with the responsibility for the state's fingerprint identification services.

State Identification Bureau (SIB) Chief — The SIB Chief is the designated manager of state's SIB. If both state fingerprint identification services and CJIS systems control are managed within the same state agency, the SIB Chief and CSO may be the same person.

State of Residency – A state of residency is the state in which an individual claims and can provide documented evidence as proof of being his/her permanent living domicile. Examples of acceptable documented evidence permitted to confirm an individual's state of residence are: driver's license, state or employer issued ID card, voter registration card, proof of an address (such as a utility bill with one's name and address as the payee), passport, professional or business license, and/or insurance (medical/dental) card.

System — Refer to connections to the FBI's criminal justice information repositories and the equipment used to establish said connections. In the context of CJI, this usually refers to applications and all interconnecting infrastructure required to use those applications that process CJI.

Tablet Devices – Tablet devices are mobile devices with a limited feature operating system (e.g. iOS, Android, Windows RT, etc.). Tablets typically consist of a touch screen without a permanently attached keyboard intended for transport via vehicle mount or portfolio-sized carry case but not on the body. This definition does not include pocket/handheld devices (e.g. smartphones) or mobile devices with full-featured operating systems (e.g. laptops).

Terminal Agency Coordinator (TAC) — Serves as the point-of-contact at the local agency for matters relating to CJIS information access. A TAC administers CJIS systems programs within the local agency and oversees the agency's compliance with CJIS systems policies.

Virtualization — Refers to a methodology of dividing the resources of a computer (hardware and software) into multiple execution environments, by applying one or more concepts or technologies such as hardware and software partitioning, time-sharing, partial or complete machine simulation or emulation allowing multiple operating systems, or images, to run concurrently on the same hardware.

Voice over Internet Protocol (VoIP) — A set of software, hardware, and standards designed to make it possible to transmit voice over packet switched networks, either an internal Local Area Network, or across the Internet.

APPENDIX B ACRONYMS

Acronym	Term
AA	Advanced Authentication
AC	Agency Coordinator
ACL	Access Control List
AES	Advanced Encryption Standard
AP	Access Point
APB	Advisory Policy Board
BD-ADDR	Bluetooth-Enabled Wireless Devices and Addresses
BYOD	Bring Your Own Device
CAD	Computer-Assisted Dispatch
CAU	CJIS Audit Unit
CFR	Code of Federal Regulations
CGA	Contracting Government Agency
CHRI	Criminal History Record Information
CJA	Criminal Justice Agency
CJI	Criminal Justice Information
CJIS	Criminal Justice Information Services
ConOps	Concept of Operations
CSA	CJIS Systems Agency
CSIRC	Computer Security Incident Response Capability
CSO	CJIS Systems Officer
DAA	Designated Approving Authority
DoJ	Department of Justice

DoJCERT	DoJ Computer Emergency Response Team
FBI	Federal Bureau of Investigation
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FOUO	For Official Use Only
HTTP	Hypertext Transfer Protocol
IAFIS	Integrated Automated Fingerprint Identification System
IDS	Intrusion Detection System
III	Interstate Identification Index
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSEC	Internet Protocol Security
ISA	Interconnection Security Agreement
ISO	Information Security Officer
IT	Information Technology
LASO	Local Agency Security Officer
LEO	Law Enforcement Online
LMR	Land Mobile Radio
MAC	Media Access Control
MCA	Management Control Agreement
MDM	Mobile Device Management
MITM	Man-in-the-Middle
MOU	Memorandum of Understanding
NCIC	National Crime Information Center

NCJA	Noncriminal Justice Agency
NICS	National Instant Criminal Background Check System
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
ORI	Originating Agency Identifier
PBX	Private Branch Exchange
PDA	Personal Digital Assistant
PII	Personally Identifiable Information
PIN	Personal Identification Number
PKI	Public Key Infrastructure
POC	Point-of-Contact
PSTN	Public Switched Telephone Network
QA	Quality Assurance
QoS	Quality of Service
RF	Radio Frequency
SA	Security Addendum
SCO	State Compact Officer
SIB	State Identification Bureau
SIG	Special Interest Group
SP	Special Publication
SPRC	Security Policy Resource Center
SSID	Service Set Identifier
TAC	Terminal Agency Coordinator
TLS	Transport Layer Security
VLAN	Virtual Local Area Network

VoIP	Voice Over Internet Protocol
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

APPENDIX C NETWORK TOPOLOGY DIAGRAMS

Network diagrams, i.e. topological drawings, are an essential part of solid network security. Through graphical illustration, a comprehensive network diagram provides the “big picture” – enabling network managers to quickly ascertain the interconnecting nodes of a network for a multitude of purposes, including troubleshooting and optimization. Network diagrams are integral to demonstrating the manner in which each agency ensures criminal justice data is afforded appropriate technical security protections and is protected during transit and at rest.

The following diagrams, labeled Appendix C.1-A through C.1-D, are examples for agencies to utilize during the development, maintenance, and update stages of their own network diagrams. By using these example drawings as a guideline, agencies can form the foundation for ensuring compliance with Section 5.7.1.2 of the CJIS Security Policy.

The purpose for including the following diagrams in this Policy is to aid agencies in their understanding of diagram expectations and should not be construed as a mandated method for network topologies. It should also be noted that agencies are not required to use the identical icons depicted in the example diagrams and should not construe any depiction of a particular vendor product as an endorsement of that product by the FBI CJIS Division.

Appendix C.1-A is a conceptual overview of the various types of agencies that can be involved in handling of CJI, and illustrates several ways in which these interconnections might occur. This diagram is not intended to demonstrate the level of detail required for any given agency’s documentation, but it provides the reader with some additional context through which to digest the following diagrams. Take particular note of the types of network interfaces in use between agencies, in some cases dedicated circuits with encryption mechanisms, and in other cases VPNs over the Internet. This diagram attempts to show the level of diversity possible within the law enforcement community. These diagrams in no way constitute a standard for network engineering, but rather, for the expected quality of documentation.

The next three topology diagrams, C.1-B through C.1-D, depict conceptual agencies. For C.1-B through C.1-D, the details identifying specific “moving parts” in the diagrams by manufacturer and model are omitted, but it is expected that any agencies producing such documentation will provide diagrams with full manufacturer and model detail for each element of the diagram. Note that the quantities of clients should be documented in order to assist the auditor in understanding the scale of assets and information being protected.

Appendix C.1-B depicts a conceptual state law enforcement agency’s network topology and demonstrates a number of common technologies that are in use throughout the law enforcement community (some of which are compulsory per CJIS policy, and some of which are optional) including Mobile Broadband cards, VPNs, Firewalls, Intrusion Detection Devices, VLANs, and so forth. Note that although most state agencies will likely have highly-available configurations, the example diagram shown omits these complexities and only shows the “major moving parts” for clarity but please note the Policy requires the logical location of all components be shown. The level of detail depicted should provide the reader with a pattern to model future documentation from, but should not be taken as network engineering guidance.

Appendix C.1-C depicts a conceptual county law enforcement agency. A number of common technologies are presented merely to reflect the diversity in the community, including proprietary

Packet-over-RF infrastructures and advanced authentication techniques, and to demonstrate the fact that agencies can act as proxies for other agencies.

Appendix C.1-D depicts a conceptual municipal law enforcement agency, presumably a small one that lacks any precinct-to-patrol data communications. This represents one of the smallest designs that could be assembled that, assuming all other details are properly considered, would meet the criteria for Section 5.7.1.2. This diagram helps to demonstrate the diversity in size that agencies handling criminal justice data exhibit.

Figure C-1-A Overview: Conceptual Connections Between Various Agencies

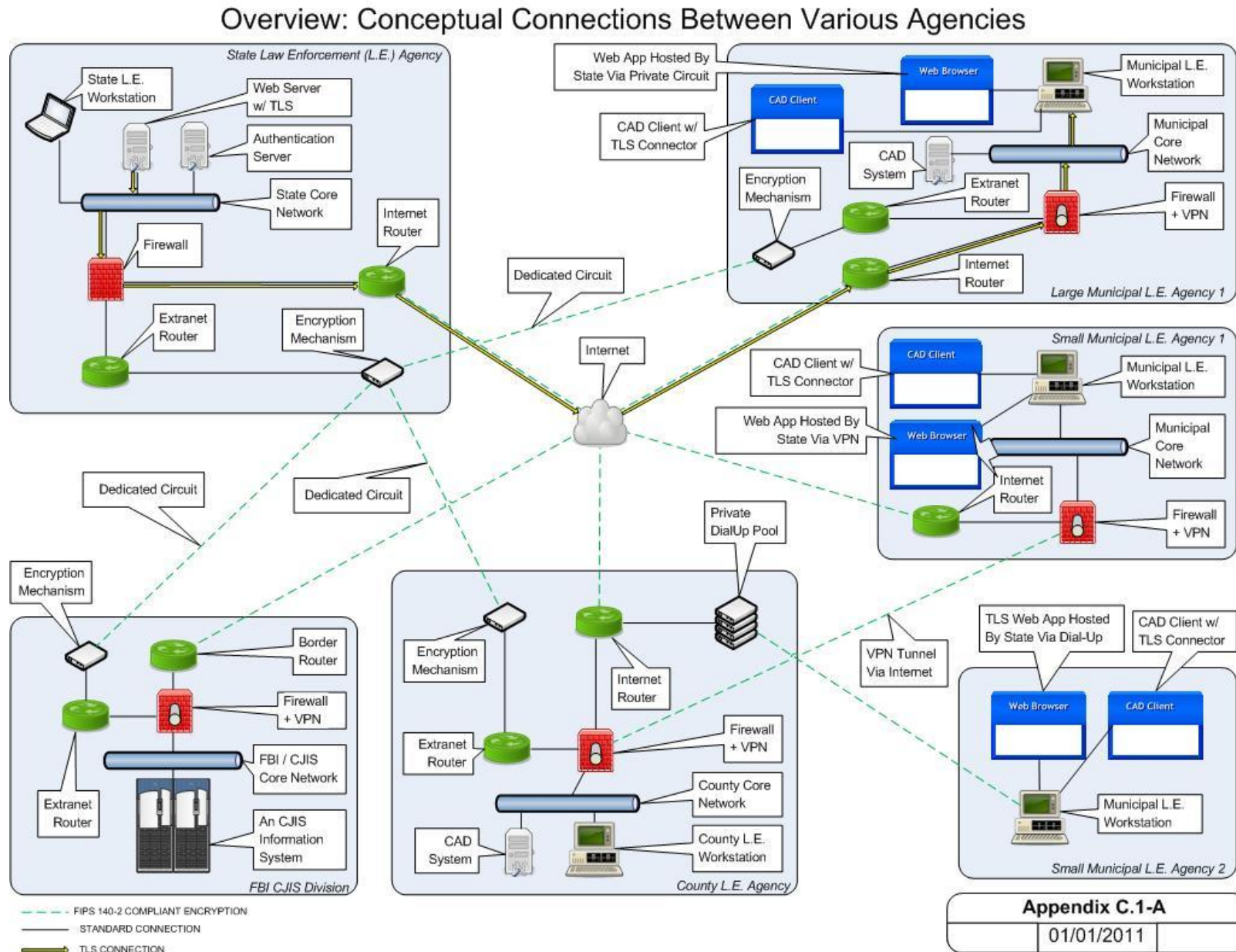
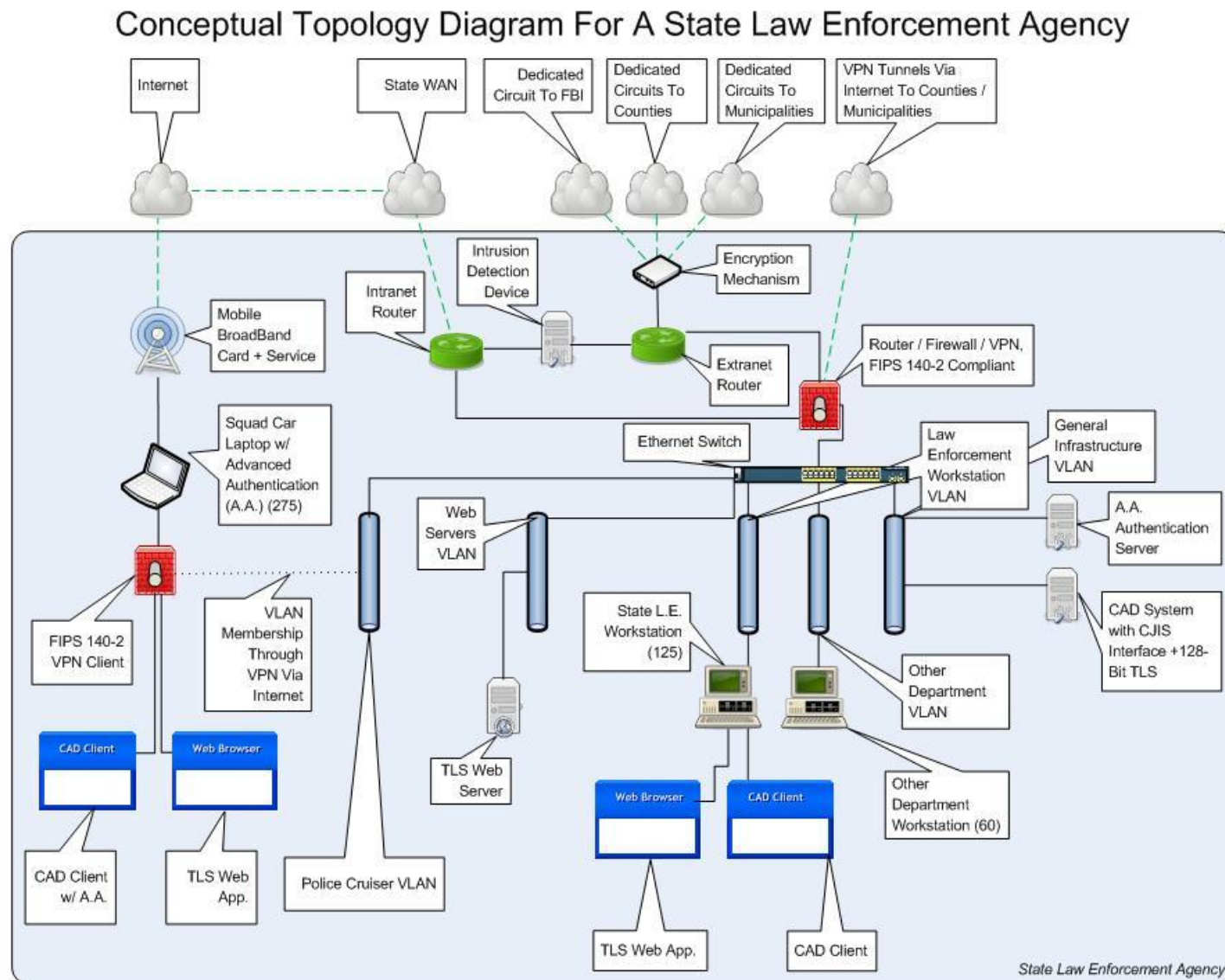


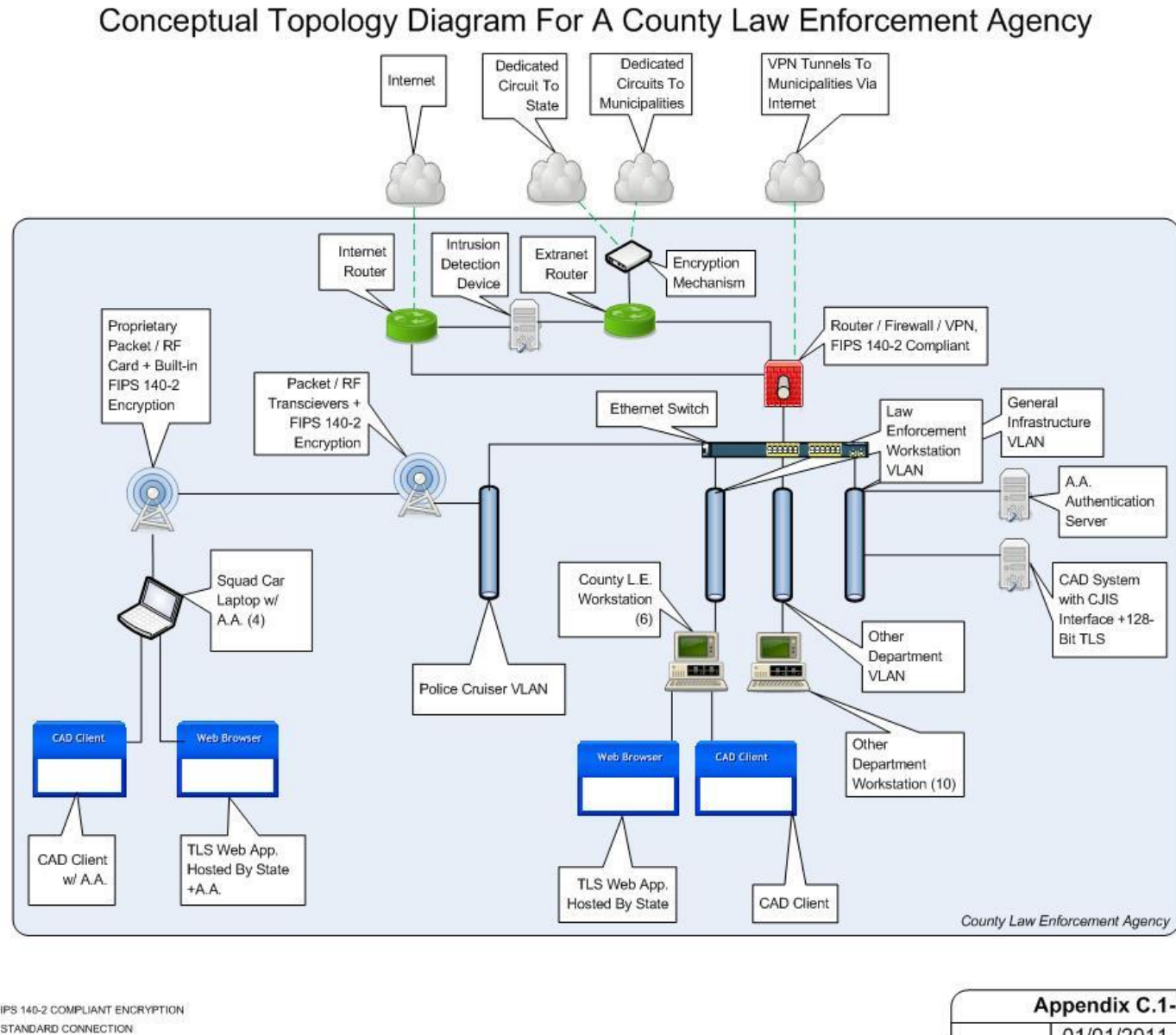
Figure C-1-B Conceptual Topology Diagram for a State Law Enforcement Agency



Appendix C.1-B

01/01/2011

Figure C-1-C Conceptual Topology Diagram for a County Law Enforcement Agency

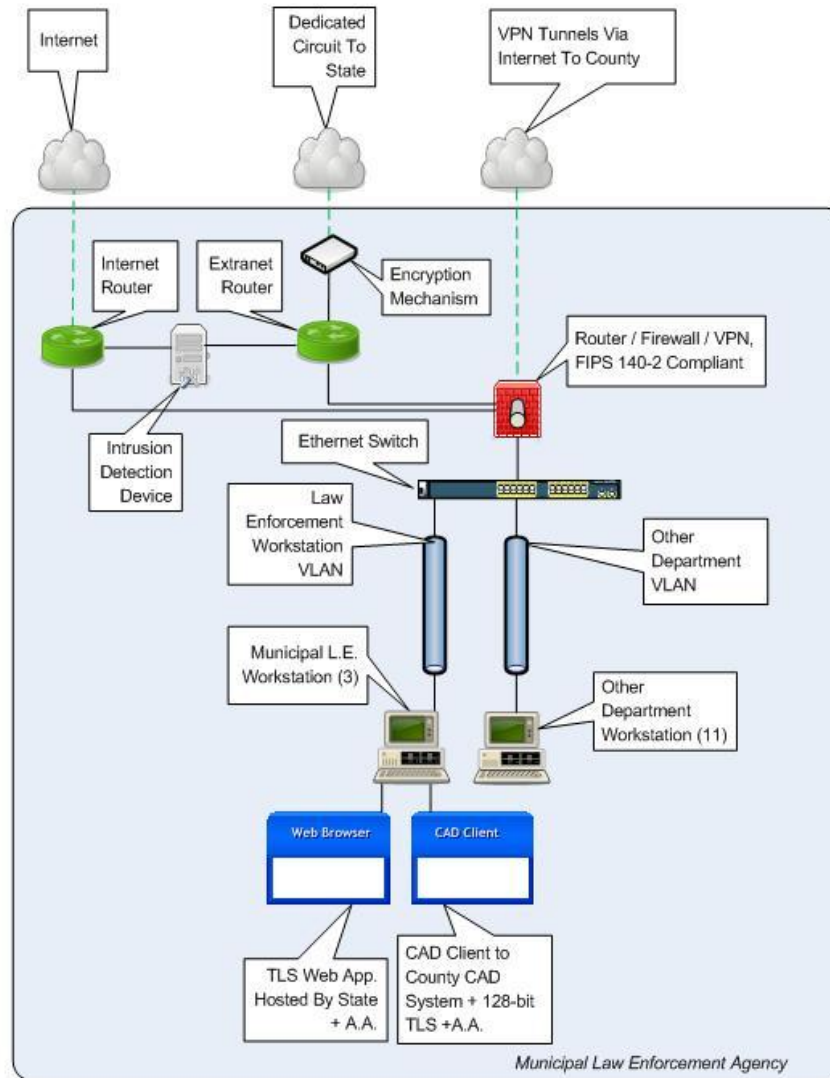


Appendix C.1-C

01/01/2011

Figure C-1-D Conceptual Topology Diagram for a Municipal Law Enforcement Agency

Conceptual Topology Diagram For A Municipal Law Enforcement Agency



--- FIPS 140-2 COMPLIANT ENCRYPTION
 — STANDARD CONNECTION

Appendix C.1-D

01/01/2011

APPENDIX D SAMPLE INFORMATION EXCHANGE AGREEMENTS

D.1 CJIS User Agreement

CRIMINAL JUSTICE INFORMATION SERVICES (CJIS) SYSTEMS USER AGREEMENT

The FBI CJIS Division provides state-of-the-art identification and information services to the local, state, tribal, federal, and international criminal justice communities, as well as the noncriminal justice community, for licensing and employment purposes. These services are administered and maintained by the FBI CJIS Division and managed in cooperation with the CJIS Systems Agency (CSA) and its administrator for CJIS data, the CJIS Systems Officer (CSO). The CJIS Systems include, but are not limited to: the Interstate Identification Index (III); National Crime Information Center (NCIC); Uniform Crime Reporting (UCR), whether summary or incident-based reporting to the National Incident-Based Reporting System; Fingerprint Identification Record System; Law Enforcement National Data Exchange (N-DEx); Law Enforcement Online; and the National Instant Criminal Background Check System (NICS).

The FBI CJIS Division provides the following services to its users, as applicable:

1. Operational, technical, and investigative assistance.
2. Telecommunication lines to state, federal, and regulatory interfaces.
3. Legal and legislative review of matters pertaining to all CJIS Systems.
4. Timely information on all aspects of all CJIS Systems and other related programs by means of operating manuals, code manuals, technical and operational updates, various newsletters, information letters, frequently asked questions, and other relevant documents.
5. Training assistance and up-to-date materials provided to each CSO, NICS Point of Contact (POC), state Compact Officer, State Administrator, Information Security Officer (ISO), and other appropriate personnel.
6. Ongoing assistance to Systems' users through meetings and briefings with the CSOs, State Administrators, Compact Officers, ISOs, and NICS State POCs to discuss operational and policy issues.
7. Advisory Process through which authorized users have input as to the policies and procedures governing the operation of CJIS programs.

8. National Crime Prevention and Privacy Compact Administrative Office through which states and other authorized users may submit issues concerning the noncriminal justice use of the III System.
9. Annual NICS Users Conference.
10. Audit.
11. Staff research assistance.

PART 1

The purpose behind a designated CSO is to unify responsibility for Systems user discipline and to ensure adherence to established procedures and policies within each signatory state/territory/tribal agency and by each federal user. This agreement outlines the responsibilities of each CSO as they relate to all CJIS Systems and other related CJIS administered programs. These individuals are ultimately responsible for planning necessary hardware, software, funding, and training for access to all CJIS Systems.

To ensure continued access as set forth above, the CSA agrees to adhere to all applicable CJIS policies including, but not limited to, the following:

1. The signatory state/tribal agency will provide fingerprints that meet submission criteria for all qualifying arrests. In addition, states/tribal agencies will make their records available for interstate exchange for criminal justice and other authorized purposes unless restricted by state/tribal law, and, where applicable, continue to move toward participation in the III and, upon ratification of the National Crime Prevention and Privacy Compact, the National Fingerprint File.
2. Appropriate and reasonable quality assurance procedures; e.g., hit confirmation, audits for record timeliness, and validation, must be in place to ensure that only complete, accurate, and valid information is maintained in the CJIS Systems.
3. Biannual file synchronization of information entered into the III by participating states.
4. Security - Each agency is responsible for appropriate security measures as applicable to physical security of terminals and telecommunication lines; personnel security to include background screening requirements; technical security to protect against unauthorized use; data security to include III use, dissemination, and logging; and security of criminal history records. Additionally, each CSO must ensure that all agencies establish an

information security structure that provides for an ISO and complies with the CJIS Security Policy.

5. Audit - Each agency shall be responsible for complying with all audit requirements for use of CJIS Systems. Each CSO is responsible for completing a triennial audit of all agencies with access to CJIS Systems through the CSO's lines.
6. Training - Each agency shall be responsible for training requirements, including compliance with operator training mandates.
7. Integrity of the Systems - Each agency shall be responsible for maintaining the integrity of the system in accordance with FBI CJIS Division/state/federal/tribal policies to ensure only authorized terminal access; only authorized transaction submission; and proper handling and dissemination of CJI. Each agency shall also be responsible for computer security incident reporting as required by the *CJIS Security Policy*.

The following documents are incorporated by reference and made part of this agreement for CSA users:

1. Bylaws for the CJIS Advisory Policy Board and Working Groups.
2. CJIS Security Policy.
3. Interstate Identification Index Operational and Technical Manual, National Fingerprint File Operations Plan, NCIC 2000 Operating Manual, UCR Handbook-NIBRS Edition, and National Incident-Based Reporting System Volumes 1, 2, and 4.
4. National Crime Prevention and Privacy Compact, 42 United States Code (U.S.C.) §14616.
5. NCIC Standards and UCR Standards, as recommended by the CJIS Advisory Policy Board.
6. The National Fingerprint File Qualification Requirements.
7. Title 28, Code of Federal Regulations, Parts 20 and 25, §50.12, and Chapter IX.
8. Electronic Fingerprint Transmission Specifications.

9. Other relevant documents, to include: NCIC Technical and Operational Updates, CJIS Information Letters, NICS User Manual, NICS Interface Control Document.
10. Applicable federal, state, and tribal laws and regulations.

PART 2

Additionally, there are authorized federal regulatory recipients and other authorized users that provide electronic fingerprint submissions through a CJIS Wide Area Network (WAN) connection (or other approved form of electronic connection) to the CJIS Division that are required to comply with the following CJIS policies:

1. The authorized user will provide fingerprints that meet submission criteria and apply appropriate and reasonable quality assurance procedures.
2. Security - Each agency is responsible for appropriate security measures as applicable to physical security of communication equipment; personnel security to include background screening requirements; technical security to protect against unauthorized use; and security of criminal history records.
3. Audit - Each authorized user shall be responsible for complying with all audit requirements for CJIS Systems. Additionally, each authorized user is subject to a triennial audit by the CJIS Division Audit staff.
4. Training - Each authorized user receiving criminal history record information shall be responsible for training requirements, including compliance with proper handling of criminal history records.

The following documents are incorporated by reference and made part of this agreement for non-CSA authorized users:

1. CJIS Security Policy.
2. National Crime Prevention and Privacy Compact, 42 U.S.C. §14616.
3. Title 28, Code of Federal Regulations, Parts 20 and 25, § 50.12, and Chapter IX.
4. Other relevant documents, to include CJIS Information Letters.

5. Applicable federal, state, and tribal laws and regulations.

GENERAL PROVISIONS

Funding:

Unless otherwise agreed in writing, each party shall bear its own costs in relation to this agreement. Expenditures will be subject to federal and state budgetary processes and availability of funds pursuant to applicable laws and regulations. The parties expressly acknowledge that this in no way implies that Congress will appropriate funds for such expenditures.

Termination:

1. All activities of the parties under this agreement will be carried out in accordance to the above-described provisions.
2. This agreement may be amended or terminated by the mutual written consent of the parties authorized representatives.
3. Either party may terminate this agreement upon 30-days written notification to the other party. Such notice will be the subject of immediate consultation by the parties to decide upon the appropriate course of action. In the event of such termination, the following rules apply:
 - a. The parties will continue participation, financial or otherwise, up to the effective date of termination.
 - b. Each party will pay the costs it incurs as a result of termination.
 - c. All information and rights therein received under the provisions of this agreement prior to the termination will be retained by the parties, subject to the provisions of this agreement.

ACKNOWLEDGMENT AND CERTIFICATION

As a CSO or CJIS WAN Official (or other CJIS authorized official), I hereby acknowledge the duties and responsibilities as set out in this agreement. I acknowledge that these duties and responsibilities have been developed and approved by CJIS Systems users to ensure the reliability, confidentiality, completeness, and accuracy of all information contained in, or obtained by means of, the CJIS Systems. I further acknowledge that failure to comply with these duties and responsibilities may result in the imposition of sanctions against the offending state/agency; other federal, tribal, state, and local criminal justice users; and approved noncriminal justice users with System access, whether direct or indirect. The Director of the FBI (or the National Crime Prevention and Privacy Compact Council), may approve sanctions to include the termination of CJIS services.

I hereby certify that I am familiar with all applicable documents that are made part of this agreement and to all applicable federal and state laws and regulations relevant to the receipt and dissemination of documents provided through the CJIS Systems.

This agreement is a formal expression of the purpose and intent of both parties and is effective when signed. It may be amended by the deletion or modification of any provision contained therein, or by the addition of new provisions, after written concurrence of both parties. The "Acknowledgment and Certification" is being executed by the CSO or CJIS WAN Official (or other CJIS authorized official) in both an individual and representative capacity. Accordingly, this agreement will remain in effect after the CSO or CJIS WAN Official (or other CJIS authorized official) vacates his/her position or until it is affirmatively amended or rescinded in writing. This agreement does not confer, grant, or authorize any rights, privileges, or obligations to any third party.

SYSTEMS USER AGREEMENT

Please execute either Part 1 or Part 2

PART 1

CJIS Systems Officer

Date: _____

Printed Name/Title

CONCURRENCE OF CSA HEAD:

CSA Head

Date: _____

Printed Name/Title

PART 2

CJIS WAN Official (or other CJIS Authorized Official)

Date: _____

Printed Name/Title

CONCURRENCE OF CJIS WAN AGENCY HEAD:

CJIS WAN Agency Head

Date: _____

Printed Name/Title

FBI CJIS DIVISION:

[Name]

Date: _____

Assistant Director

FBI CJIS Division

* The FBI Designated Federal Officer should be notified when a CSO or other CJIS WAN/authorized Official vacates his/her position. The name and telephone number of the Acting CSO or other CJIS WAN/authorized Official, and when known, the name and telephone number of the new CSO or other CJIS WAN/authorized Official, should be provided. Revised: 05/03/2006

D.2 Management Control Agreement

Management Control Agreement

Pursuant to the CJIS Security Policy, it is agreed that with respect to administration of that portion of computer systems and network infrastructure interfacing directly or indirectly with the state network (Network Name) for the interstate exchange of criminal history/criminal justice information, the (Criminal Justice Agency) shall have the authority, via managed control, to set, maintain, and enforce:

- (1) Priorities.
- (2) Standards for the selection, supervision, and termination of personnel access to Criminal Justice Information (CJI).
- (3) Policy governing operation of justice systems, computers, access devices, circuits, hubs, routers, firewalls, and any other components, including encryption, that comprise and support a telecommunications network and related criminal justice systems to include but not limited to criminal history record/criminal justice information, insofar as the equipment is used to process or transmit criminal justice systems information guaranteeing the priority, integrity, and availability of service needed by the criminal justice community.
- (4) Restriction of unauthorized personnel from access or use of equipment accessing the State network.
- (5) Compliance with all rules and regulations of the (Criminal Justice Agency) Policies and CJIS Security Policy in the operation of all information received.

“...management control of the criminal justice function remains solely with the Criminal Justice Agency.” Section 5.1.1.4

This agreement covers the overall supervision of all (Criminal Justice Agency) systems, applications, equipment, systems design, programming, and operational procedures associated with the development, implementation, and maintenance of any (Criminal Justice Agency) system to include NCIC Programs that may be subsequently designed and/or implemented within the (Criminal Justice Agency).

John Smith, CIO
Any State Department of Administration

Date

Joan Brown, CIO
(Criminal Justice Agency)

Date

D.3 Noncriminal Justice Agency Agreement & Memorandum of Understanding

MEMORANDUM OF UNDERSTANDING

BETWEEN

THE FEDERAL BUREAU OF INVESTIGATION

AND

(Insert Name of Requesting Organization)

FOR

THE ESTABLISHMENT AND ACCOMMODATION OF
THIRD-PARTY CONNECTIVITY TO THE
CRIMINAL JUSTICE INFORMATION SERVICES DIVISION'S WIDE AREA NETWORK

1. **PURPOSE:** This Memorandum of Understanding (MOU) between the Federal Bureau of Investigation (FBI) and **(insert requesting organization's name)**, hereinafter referred to as the "parties," memorializes each party's responsibilities with regard to establishing connectivity to records services accessible via the Wide Area Network (WAN) of the FBI's Criminal Justice Information Services (CJIS) Division.

2. **BACKGROUND:** The requesting organization, **(insert requesting organization's name)**, being approved for access to systems of records accessible via the CJIS WAN, desires connectivity to the CJIS WAN or via a secure Virtual Private Network (VPN) Connection (Internet) to the CJIS WAN. The CJIS Division has created a framework for accommodating such requests based on the type of connection.

In preparing for such non-CJIS-funded connectivity to the CJIS WAN, the parties plan to acquire, configure, and place needed communications equipment at suitable sites and to make electronic connections to the appropriate systems of records via the CJIS WAN.

To ensure that there is a clear understanding between the parties regarding their respective roles in this process, this MOU memorializes each party's responsibilities regarding the development, operation, and maintenance of third-party connectivity to the CJIS WAN. Unless otherwise contained in an associated contract, the enclosed terms apply. If there is a conflict between terms and provisions contained in both the contract and this MOU, the contract will prevail.

3. **AUTHORITY:** The FBI is entering into this MOU under the authority provided by Title 28, United States Code (U.S.C.), Section 534; 42 U.S.C. § 14616; and/or Title 28, Code of Federal Regulations, Part 906.

4. SCOPE:

a. The CJIS Division agrees to:

i. Provide the requesting organization with a "CJIS WAN Third-Party Connectivity Package" that will detail connectivity requirements and options compatible with the CJIS Division's WAN architecture upon receipt of a signed nondisclosure statement.

ii. Configure the requesting organization's connection termination equipment suite at Clarksburg, West Virginia, and prepare it for deployment or shipment under the CJIS WAN option. In the Secure VPN arrangement only, the third party will develop, configure, manage, and maintain its network connectivity to its preferred service provider.

iii. Work with the requesting organization to install the connection termination equipment suite and verify connectivity.

iv. Perform installation and/or routine maintenance on the requesting organization's third-party dedicated CJIS WAN connection termination equipment after coordinating with the requesting organization's designated point of contact (POC) and during a time when the CJIS Division's technical personnel are near the requesting organization's site.

v. Perform periodic monitoring and troubleshooting of the requesting organization's CJIS WAN connection termination equipment. Software patches will be maintained on the dedicated CJIS WAN connected network equipment only. Under the Secure VPN option, no availability or data thru-put rates will be guaranteed.

vi. Provide 24 hours a day, 7 days a week uninterrupted monitoring from the CJIS Division's Network Operations Center.

vii. Provide information regarding potential hardware end-of-life replacement cycles to the requesting organization for its budgeting purposes.

viii. Maintain third-party dedicated CJIS WAN connection termination equipment as if in the CJIS Division's operational environment.

ix. Update the appropriate software on the requesting organization's dedicated connection termination equipment connected to the CJIS WAN (i.e., Cisco Internetwork Operating System, SafeNet frame relay encryptor firmware, etc.) pursuant to the requesting organization's authorized maintenance contracts.

x. Provide a POC and telephone number for MOU-related issues.

b. The **(insert requesting organization's name)** agrees to:

i. Coordinate requests for third-party connectivity to the CJIS WAN or the Secure VPN with the CJIS Division's POC.

ii. Purchase hardware and software that are compatible with the CJIS WAN.

iii. Pay for the telecommunications infrastructure that supports its connection to the CJIS WAN or Secure VPN.

iv. Maintain telecommunication infrastructure in support of Secure VPN connectivity.

v. Provide any/all hardware and software replacements and upgrades as mutually agreed to by the parties.

vi. Pay for all telecommunication requirements related to its connectivity.

vii. Provide required information for dedicated service relating to Data Link Connection Identifiers, Circuit Identifier, Permanent Virtual Circuit Identifiers, Local Exchange Carrier Identifier, POC, location, etc., as determined by the parties.

viii. Transport the CJIS WAN connection termination equipment suite to the CJIS Division for configuration and preparation for deployment under the dedicated service option.

ix. Provide registered Internet Protocol information to be used by the requesting organization's system to the CJIS Division.

x. Provide the CJIS Division with six months advance notice or stated amount of time for testing activities (i.e., disaster recovery exercises).

xi. Provide the CJIS Division with applicable equipment maintenance contract numbers and level of service verifications needed to perform software upgrades on connection termination equipment.

xii. Provide the CJIS Division with applicable software upgrade and patch images (or information allowing the CJIS Division to access such images).

xiii. Transport only official, authorized traffic over the Secure VPN.

xiv. Provide a POC and telephone number for MOU-related issues.

5. FUNDING: There are no reimbursable expenses associated with this level of support. Each party will fund its own activities unless otherwise agreed to in writing. This MOU is not an obligation or commitment of funds, nor a basis for transfer of funds, but rather is a basic statement of understanding between the parties hereto of the nature of the relationship for the connectivity efforts. Unless otherwise agreed to in writing, each party shall bear its own costs in relation to this MOU. Expenditures by each party will be subject to its budgetary processes and to the availability of funds and resources pursuant to applicable laws, regulations, and policies. The parties expressly acknowledge that the above language in no way implies that Congress will appropriate funds for such expenditures.

6. SETTLEMENT OF DISPUTES: Disagreements between the parties arising under or relating to this MOU will be resolved only by consultation between the parties and will not be referred to any other person or entity for settlement.

7. SECURITY: It is the intent of the parties that the actions carried out under this MOU will be conducted at the unclassified level. No classified information will be provided or generated under this MOU.

8. AMENDMENT, TERMINATION, ENTRY INTO FORCE, AND DURATION:

a. All activities of the parties under this MOU will be carried out in accordance with the above - described provisions.

b. This MOU may be amended or terminated by the mutual written consent of the parties' authorized representatives.

c. Either party may terminate this MOU upon 30-days written notification to the other party. Such notice will be the subject of immediate consultation by the parties to decide upon the appropriate course of action. In the event of such termination, the following rules apply:

i. The parties will continue participation, financial or otherwise, up to the effective date of the termination.

ii. Each party will pay the costs it incurs as a result of the termination.

iii. All information and rights therein received under the provisions of this MOU prior to the termination will be retained by the parties, subject to the provisions of this MOU.

9. FORCE AND EFFECT: This MOU, which consists of nine numbered sections, will enter into effect upon signature of the parties and will remain in effect until terminated. The parties should review the contents of this MOU annually to determine whether there is a need for the deletion, addition, or amendment of any provision. This MOU is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable at law or otherwise by any third party against the parties, their parent agencies, the United States, or the officers, employees, agents, or other associated personnel thereof.

The foregoing represents the understandings reached between the parties.

FOR THE FEDERAL BUREAU OF INVESTIGATION

[Name]

Date

Assistant Director

Criminal Justice Information Services Division

FOR THE (insert requesting organization name)

Date

D.4 Interagency Connection Agreement

CRIMINAL JUSTICE INFORMATION SERVICES (CJIS)

Wide Area Network (WAN) USER AGREEMENT

BY INTERIM REMOTE LATENT USERS

The responsibility of the FBI CJIS Division is to provide state-of-the-art identification and information services to the local, state, federal, and international criminal justice communities, as well as the civil community for licensing and employment purposes. The data provided by the information systems administered and maintained by the FBI CJIS Division are routed to and managed in cooperation with the designated interface agency official. This information includes, but is not limited to, the Interstate Identification Index (III), National Crime Information Center (NCIC), Uniform Crime Reporting (UCR)/National Incident-Based Reporting System (NIBRS), and the Integrated Automated Fingerprint Identification System (IAFIS) programs.

In order to fulfill this responsibility, the FBI CJIS Division provides the following services to its users:

- Operational, technical, and investigative assistance;
- Telecommunications lines to local, state, federal and authorized interfaces;
- Legal and legislative review of matters pertaining to IAFIS, CJIS WAN and other related services;
- Timely information on all aspects of IAFIS, CJIS WAN, and other related programs by means of technical and operational updates, various newsletters, and other relative documents;
- Shared management through the CJIS Advisory Process and the Compact Council;
- Training assistance and up-to-date materials provided to each designated agency official, and;

- Audit.

The concept behind a designated interface agency official is to unify responsibility for system user discipline and ensure adherence to system procedures and policies within each interface agency. These individuals are ultimately responsible for planning necessary hardware, software, funding, training, and the administration of policy and procedures including security and integrity for complete access to CJIS related systems and CJIS WAN related data services by authorized agencies.

The following documents and procedures are incorporated by reference and made part of this agreement:

- *CJIS Security Policy*;
- *Title 28, Code of Federal Regulations, Part 20*;
- Computer Incident Response Capability (CIRC);
- Applicable federal and state laws and regulations.

To ensure continued access as set forth above, the designated interface agency agrees to adhere to all CJIS policies, including, but not limited to, the following:

1. The signatory criminal agency will provide fingerprints for all qualifying arrests either via electronic submission or fingerprint card that meet submission criteria. In addition, the agency will make their records available for interstate exchange for criminal justice and other authorized purposes.
2. The signatory civil agency with legislative authority will provide all qualifying fingerprints via electronic submission or fingerprint card that meet submission criteria.
3. Appropriate and reasonable quality assurance procedures must be in place to ensure that only complete, accurate, and valid information is maintained in the system.

4. Security - Each agency is responsible for appropriate security measures as applicable to physical security of terminals and telecommunications lines; Interim Distributed Imaging System (IDIS) equipment shall remain stand-alone devices and be used only for authorized purposes; personnel security to meet background screening requirements; technical security to protect against unauthorized use; data security, dissemination, and logging for audit purposes; and actual security of criminal history records. Additionally, each agency must establish an information security structure that provides for an Information Security Officer (ISO) or a security point of contact.
5. Audit - Each agency shall be responsible for complying with the appropriate audit requirements.
6. Training - Each agency shall be responsible for training requirements, including compliance with training mandates.
7. Integrity of the system shall be in accordance with FBI CJIS Division and interface agency policies. Computer incident reporting shall be implemented.

Until states are able to provide remote latent connectivity to their respective latent communities via a state WAN connection, the CJIS Division may provide direct connectivity to IAFIS via a dial-up connection or through the Combined DNA Index System (CODIS) and/or National Integrated Ballistics Information Network (NIBIN) connections. When a state implements a latent management system and is able to provide intrastate connectivity and subsequent forwarding to IAFIS, this agreement may be terminated. Such termination notice will be provided in writing by either the FBI or the state CJIS Systems Agency.

It is the responsibility of the local remote latent user to develop or acquire an IAFIS compatible workstation. These workstations may use the software provided by the FBI or develop their own software, provided it is IAFIS compliant.

The CJIS Division will provide the approved modem and encryptors required for each dial-up connection to IAFIS. The CJIS Communication Technologies Unit will configure and test the encryptors before they are provided to the user. Users requesting remote latent connectivity through an existing CODIS and/or NIBIN connection must receive verification from the FBI that there are a sufficient number of Ethernet ports on the router to accommodate the request.

If at any time search limits are imposed by the CJIS Division, these individual agency connections will be counted toward the total state allotment.

ACKNOWLEDGMENT AND CERTIFICATION

As a CJIS WAN interface agency official serving in the CJIS system, I hereby acknowledge the duties and responsibilities as set out in this agreement. I acknowledge that these duties and responsibilities have been developed and approved by CJIS system users in order to ensure the reliability, confidentiality, completeness, and accuracy of all information contained in or obtained by means of the CJIS system. I further acknowledge that a failure to comply with these duties and responsibilities may subject our agency to various sanctions adopted by the CJIS Advisory Policy Board and approved by the Director of the FBI. These sanctions may include the termination of CJIS service.

As the designated CJIS WAN interface agency official serving in the CJIS system, I hereby certify that I am familiar with the contents of the *Title 28, Code of Federal Regulations, Part 20; CJIS Security Policy; Computer Incident Response Capability*; and applicable federal or state laws and regulations applied to IAFIS and CJIS WAN Programs for the dissemination of criminal history records for criminal and noncriminal justice purposes.

*

Signature

Print or Type

CJIS WAN Agency Official

Date

CONCURRENCE OF FEDERAL/REGULATORY AGENCY HEAD OR STATE CJIS SYSTEMS OFFICER (CSO):

*

Signature

Print or Type

*

Title

Date

State CSO

FBI CJIS DIVISION:

Signature – [Name]

Assistant Director

Title

Date

* If there is a change in the CJIS WAN interface agency official, the FBI Designated Federal Employee must be notified in writing 30 days prior to the change.

5/27/2004 UA modification reflects change in CTO title to CSO.

APPENDIX E SECURITY FORUMS AND ORGANIZATIONAL ENTITIES

Online Security Forums / Organizational Entities
AntiOnline
Black Hat
CIO.com
CSO Online
CyberSpeak Podcast
FBI Criminal Justice Information Services Division (CJIS)
Forrester Security Forum
Forum of Incident Response and Security Teams (FIRST)
Information Security Forum (ISF)
Information Systems Audit and Control Association (ISACA)
Information Systems Security Association (ISSA)
Infosyssec
International Organization for Standardization (ISO)
International Information Systems Security Certification Consortium, Inc. (ISC) ²
Metasploit
Microsoft Developer Network (MSDN) Information Security
National Institute of Standards and Technology (NIST)
Open Web Application Security Project (OWASP)
SANS (SysAdmin, Audit, Network, Security) Institute
SC Magazine
Schneier.com
Security Focus
The Register
US Computer Emergency Response Team (CERT)
US DoJ Computer Crime and Intellectual Property Section (CCIPS)

APPENDIX F SAMPLE FORMS

This appendix contains sample forms.

F.1 IT Security Incident Response Form

FBI CJIS DIVISION

INFORMATION SECURITY OFFICER (ISO)

COMPUTER SECURITY INCIDENT RESPONSE CAPABILITY (CSIRC)

REPORTING FORM

DATE OF REPORT: _____ (mm/dd/yyyy)

DATE OF INCIDENT: _____ (mm/dd/yyyy)

POINT(S) OF CONTACT: _____ PHONE/EXT/E-MAIL: _____

LOCATION(S) OF INCIDENT: _____

SYSTEM(S) AFFECTED: _____

AFFECTED SYSTEM(S) DESCRIPTION (e.g. CAD, RMS, file server, etc.): _____

METHOD OF DETECTION: _____

NATURE OF INCIDENT: _____

INCIDENT DESCRIPTION: _____

ACTIONS TAKEN/RESOLUTION: _____

Copies To:

George White

(FBI CJIS Division ISO)

1000 Custer Hollow Road

Clarksburg, WV 26306-0102

(304) 625-5849

iso@leo.gov

George White

(FBI CJIS CSIRC POC)

1000 Custer Hollow Road/Module D-2

Clarksburg, WV 26306-0102

(304) 625-5849

iso@leo.gov

APPENDIX G BEST PRACTICES

G.1 Virtualization

Virtualization

This appendix documents security considerations for implementing and operating virtual environments that process, store, and/or transmit Criminal Justice Information.

The FBI CJIS ISO has fielded several inquiries from various states requesting guidance on implementing virtual environments within their data centers. With the proliferation of virtual environments across industry in general there is a realistic expectation that FBI CJIS Auditors will encounter virtual environments during the upcoming year. Criminal Justice Agencies (CJAs) and Noncriminal Justice Agencies (NCJAs) alike need to understand and appreciate the foundation of security protection measures required for virtual environments.

From Microsoft's Introduction to Windows Server 2008

<http://www.microsoft.com/windowsserver2008/en/us/hyperv.aspx>:

"Server virtualization, also known as hardware virtualization, is a hot topic in the IT world because of the potential for serious economic benefits. Server virtualization enables multiple operating systems to run on a single physical machine as virtual machines (VMs). With server virtualization, you can consolidate workloads across multiple underutilized server machines onto a smaller number of machines. Fewer physical machines can lead to reduced costs through lower hardware, energy, and management overhead, plus the creation of a more dynamic IT infrastructure."

From a trade publication, kernelthread.com

<http://www.kernelthread.com/publications/virtualization/>:

"Virtualization is a framework or methodology of dividing the resources of a computer into multiple execution environments, by applying one or more concepts or technologies such as hardware and software partitioning, time-sharing, partial or complete machine simulation, emulation, quality of service, and many others."

From an Open Source Software developer

<http://www.kallasoft.com/pc-hardware-virtualization-basics/>:

"Virtualization refers to virtualizing hardware in software, allowing multiple operating systems, or images, to run concurrently on the same hardware. There are two main types of virtualization software:

- *"Type-1 Hypervisor, which runs 'bare-metal' (on top of the hardware)*
- *"Type-2 Hypervisor which requires a separate application to run within an operating system*

“Type1 hypervisors usually offer the best in efficiency, while Type-2 hypervisors allow for greater support of hardware that can be provided by the operating system. For the developer, power user, and small business IT professionals, virtualization offers the same basic idea of collapsing multiple physical boxes into one. For instance, a small business can run a web server and an Exchange server without the need for two boxes. Developers and power users can use the ability to contain different development environments without the need to modify their main operating system. Big businesses can also benefit from virtualization by allowing software maintenance to be run and tested on a separate image on hardware without having to take down the main production system.”

Industry leaders and niche developers are bringing more products to market every day. The following article excerpts, all posted during September 2008, on www.virtualization.com are examples of industry offerings.

“Microsoft and Novell partnered together for joint virtualization solution. Microsoft and Novell are announcing the availability of a joint virtualization solution optimized for customers running mixed-source environments. The joint offering includes SUSE Linux Enterprise Server configured and tested as an optimized guest operating system running on Windows Server 2008 Hyper-V, and is fully supported by both companies’ channel partners. The offering provides customers with the first complete, fully supported and optimized virtualization solution to span Windows and Linux environments.”

“Sun Microsystems today announce the availability of Sun xVM Server software and Sun xVM Ops Center 2.0, key components in its strategy. Sun also announced the addition of comprehensive services and support for Sun xVM Server software and xVM Ops Center 2.0 to its virtualization suite of services. Additionally, Sun launched xVMserver.org, a new open source community, where developers can download the first source code bundle for Sun xVM Server software and contribute to the direction and development of the product.”

“NetEx, specialist in high-speed data transport over TCP, today announced Virtual HyperIP bandwidth optimization solutions for VMware environments that deliver a threefold to tenfold increase in data replication performance. Virtual HyperIP is a software-based Data Transport Optimizer that operates on the VMware ESX server and boosts the performance of storage replication applications from vendors such as EMC, NetApp, Symantec, IBM, Data Domain, and FalconStor. Virtual HyperIP mitigates TCP performance issues that are common when moving data over wide-area network (WAN) connections because of bandwidth restrictions, latency due to distance and/or router hop counts, packet loss and network errors. Like the company’s award-winning appliance-based HyperIP, Virtual HyperIP eliminates these issues with an innovative software design developed specifically to accelerate traffic over an IP based network.”

From several sources, particularly:

<http://www.windowsecurity.com/articles/security-virtualization.html>

<http://csrc.nist.gov/publications/drafts/6--64rev2/draft-sp800-64-Revision2.pdf>

Virtualization provides several benefits:

- Make better use of under-utilized servers by consolidating to fewer machines saving on hardware, environmental costs, management, and administration of the server infrastructure.
- Legacy applications unable to run on newer hardware and/or operating systems can be loaded into a virtual environment – replicating the legacy environment.
- Provides for isolated portions of a server where trusted and untrusted applications can be ran simultaneously – enabling hot standbys for failover.
- Enables existing operating systems to run on shared memory multiprocessors.
- System migration, backup, and recovery are easier and more manageable.

Virtualization also introduces several vulnerabilities:

- Host Dependent.
- If the host machine has a problem then all the VMs could potentially terminate.
- Compromise of the host makes it possible to take down the client servers hosted on the primary host machine.
- If the virtual network is compromised then the client is also compromised.
- Client share and host share can be exploited on both instances. Potentially this can lead to files being copied to the share that fill up the drive.

These vulnerabilities can be mitigated by the following factors:

- Apply “least privilege” technique to reduce the attack surface area of the virtual environment and access to the physical environment.
- Configuration and patch management of the virtual machine and host, i.e. Keep operating systems and application patches up to date on both virtual machines and hosts.
- Install the minimum applications needed on host machines.
- Practice isolation from host and virtual machine.
- Install and keep updated antivirus on virtual machines and the host.
- Segregation of administrative duties for host and versions.
- Audit logging as well as exporting and storing the logs outside the virtual environment.
- Encrypting network traffic between the virtual machine and host IDS and IPS monitoring.
- Firewall each virtual machine from each other and ensure that only allowed protocols will transact.

G.2 Voice over Internet Protocol White Paper

Voice over Internet Protocol (VoIP)

Attribution:

The following information has been extracted from NIST Special Publication 800-58, Security Considerations for Voice over IP Systems.

Definitions:

Voice over Internet Protocol (VoIP) – A set of software, hardware, and standards designed to make it possible to transmit voice over packet switched networks, either an internal Local Area Network, or across the Internet.

Internet Protocol (IP) - A protocol used for communicating data across a packet-switched internetwork using the Internet Protocol Suite, also referred to as TCP/IP. IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering distinguished protocol datagrams (packets) from the source host to the destination host solely based on their addresses.

Summary:

Voice over Internet Protocol (VoIP) has been embraced by organizations globally as an addition to, or replacement for, public switched telephone network (PSTN) and private branch exchange (PBX) telephone systems. The immediate benefits are alluring since the typical cost to operate VoIP is less than traditional telephone services and VoIP can be installed in-line with an organization's existing Internet Protocol services. Unfortunately, installing a VoIP network is not a simple "plug-and-play" procedure. There are myriad security concerns, cost issues with new networking hardware requirements, and overarching quality of service (QoS) factors that have to be considered carefully.

What are some of the advantages of VoIP?

- a. Cost – a VoIP system is usually cheaper to operate than an equivalent office telephone system with a Private Branch Exchange and conventional telephone service.
- b. Integration with other services – innovative services are emerging that allow customers to combine web access with telephone features through a single PC or terminal. For example, a sales representative could discuss products with a customer

using the company's web site. In addition, the VoIP system may be integrated with video across the Internet, providing a teleconferencing facility.

What are some of the disadvantages of VoIP?

- a. Startup cost – although VoIP can be expected to save money in the long run, the initial installation can be complex and expensive. In addition, a single standard has not yet emerged for many aspects of VoIP, so an organization must plan to support more than one standard, or expect to make relatively frequent changes as the VoIP field develops.
- b. Security – the flexibility of VoIP comes at a price: added complexity in securing voice and data. Because VoIP systems are connected to the data network, and share many of the same hardware and software components, there are more ways for intruders to attack a VoIP system than a conventional voice telephone system or PBX.

VoIP Risks, Threats, and Vulnerabilities

This section details some of the potential threats and vulnerabilities in a VoIP environment, including vulnerabilities of both VoIP phones and switches. Threat discussion is included because the varieties of threats faced by an organization determine the priorities in securing its communications equipment. Not all threats are present in all organizations. A commercial firm may be concerned primarily with toll fraud, while a government agency may need to prevent disclosure of sensitive information because of privacy or national security concerns. Information security risks can be broadly categorized into the following three types: confidentiality, integrity, and availability, (which can be remembered with the mnemonic "CIA"). Additional risks relevant to switches are fraud and risk of physical damage to the switch, physical network, or telephone extensions.

Packet networks depend for their successful operation on a large number of configurable parameters: IP and MAC (physical) addresses of voice terminals, addresses of routers and firewalls, and VoIP specific software such as Call Managers and other programs used to place and route calls. Many of these network parameters are established dynamically every time a network component is restarted, or when a VoIP telephone is restarted or added to the network. Because there are so many places in a network with dynamically configurable parameters, intruders have a wide array of potentially vulnerable points to attack.

Vulnerabilities described in this section are generic and may not apply to all systems, but investigations by NIST and other organizations have found these vulnerabilities in a number of VoIP systems. In addition, this list is not exhaustive; systems may have security weaknesses that are not included in the list. For each potential vulnerability, a recommendation is included to eliminate or reduce the risk of compromise.

Confidentiality and Privacy

Confidentiality refers to the need to keep information secure and private. For home computer users, this category includes confidential memoranda, financial information, and security information such as passwords. In a telecommunications switch,

eavesdropping on conversations is an obvious concern, but the confidentiality of other information on the switch must be protected to defend against toll fraud, voice and data interception, and denial of service attacks. Network IP addresses, operating system type, telephone extension to IP address mappings, and communication protocols are all examples of information that, while not critical as individual pieces of data, can make an attacker's job easier

With conventional telephones, eavesdropping usually requires either physical access to tap a line, or penetration of a switch. Attempting physical access increases the intruder's risk of being discovered, and conventional PBXs have fewer points of access than VoIP systems. With VoIP, opportunities for eavesdroppers increase dramatically, because of the many nodes in a packet network.

Switch Default Password Vulnerability

It is common for switches to have a default login/password set, e.g., admin/admin, or root/root. This vulnerability also allows for wiretapping conversations on the network with port mirroring or bridging. An attacker with access to the switch administrative interface can mirror all packets on one port to another, allowing the indirect and unnoticeable interception of all communications. Failing to change default passwords is one of the most common errors made by inexperienced users.

REMEDIATION: If possible, remote access to the graphical user interface should be disabled to prevent the interception of plaintext administration sessions. Some devices provide the option of a direct USB connection in addition to remote access through a web browser interface. Disabling port mirroring on the switch should also be considered.

Classical Wiretap Vulnerability

Attaching a packet capture tool or protocol analyzer to the VoIP network segment makes it easy to intercept voice traffic.

REMEDIATION: A good physical security policy for the deployment environment is a general first step to maintaining confidentiality. Disabling the hubs on IP Phones as well as developing an alarm system for notifying the administrator when an IP Phone has been disconnected will allow for the possible detection of this kind of attack.

ARP Cache Poisoning and ARP Floods

Because many systems have little authentication, an intruder may be able to log onto a computer on the VoIP network segment, and then send ARP commands corrupting ARP caches on sender(s) of desired traffic, then activate IP. An ARP flood attack on the switch could render the network vulnerable to conversation eavesdropping. Broadcasting ARP replies blind is sufficient to corrupt many ARP caches. Corrupting the ARP cache makes it possible to re-route traffic to intercept voice and data traffic.

REMEDIATION: Use authentication mechanisms wherever possible and limit physical access to the VoIP network segment.

Web Server interfaces

Both VoIP switches and voice terminals are likely to have a web server interface for remote or local administration. An attacker may be able to sniff plaintext HTTP packets to gain confidential information. This would require access to the local network on which the server resides.

REMEDIATION: If possible, do not use an HTTP server. If it is necessary to use a web server for remote administration, use the more secure HTTPS (HTTP over SSL or TLS) protocol.

IP Phone Netmask Vulnerability

A similar effect of the ARP Cache Vulnerability can be achieved by assigning a subnet mask and router address to the phone crafted to cause most or all of the packets it transmits to be sent to an attacker's MAC address. Again, standard IP forwarding makes the intrusion all but undetectable.

REMEDIATION: A firewall filtering mechanism can reduce the probability of this attack. Remote access to IP phones is a severe risk.

Extension to IP Address Mapping Vulnerability

Discovering the IP address corresponding to any extension requires only calling that extension and getting an answer. A protocol analyzer or packet capture tool attached to the hub on the dialing instrument will see packets directly from the target instrument once the call is answered. Knowing the IP address of a particular extension is not a compromise in itself, but makes it easier to accomplish other attacks. For example, if the attacker is able to sniff packets on the local network used by the switch, it will be easy to pick out packets sent and received by a target phone. Without knowledge of the IP address of the target phone, the attacker's job may be much more difficult to accomplish and require much longer, possibly resulting in the attack being discovered.

REMEDIATION: Disabling the hub on the IP Phone will prevent this kind of attack. However, it is a rather simple task to turn the hub back on.

Integrity Issues

Integrity of information means that information remains unaltered by unauthorized users. For example, most users want to ensure that bank account numbers cannot be changed by anyone else, or that passwords are changed only by the user or an authorized security administrator. Telecommunication switches must protect the integrity of their system data and configuration. Because of the richness of feature sets available on switches, an attacker who can compromise the system configuration can accomplish nearly any other goal. For example, an ordinary extension could be re-assigned into a pool of phones that supervisors can listen in on or record conversations for quality control purposes. Damaging or deleting information about the IP network used by a VoIP switch results in an immediate denial of service.

The security system itself provides the capabilities for system abuse and misuse. That is, compromise of the security system not only allows system abuse but also allows the elimination of all traceability and the insertion of trapdoors for intruders to use on their

next visit. For this reason, the security system must be carefully protected. Integrity threats include any in which system functions or data may be corrupted, either accidentally or as a result of malicious actions. Misuse may involve legitimate users (i.e. insiders performing unauthorized operations) or intruders.

A legitimate user may perform an incorrect, or unauthorized, operations function (e.g., by mistake or out of malice) and may cause deleterious modification, destruction, deletion, or disclosure of switch software and data. This threat may be caused by several factors including the possibility that the level of access permission granted to the user is higher than what the user needs to remain functional.

Intrusion - An intruder may masquerade as a legitimate user and access an operations port of the switch. There are a number of serious intrusion threats. For example, the intruder may use the permission level of the legitimate user and perform damaging operations functions such as:

- Disclosing confidential data
- Causing service deterioration by modifying the switch software
- Crashing the switch
- Removing all traces of the intrusion (e.g., modifying the security log) so that it may not be readily detected

Insecure state - At certain times the switch may be vulnerable due to the fact that it is not in a secure state. For example:

- After a system restart, the old security features may have been reset to insecure settings, and new features may not yet be activated. (For example, all old passwords may have reverted to the default system-password, even though new passwords are not yet assigned.) The same may happen at the time of a disaster recovery.
- At the time of installation the switch may be vulnerable until the default security features have been replaced.

DHCP Server Insertion Attack

It is often possible to change the configuration of a target phone by exploiting the DHCP response race when the IP phone boots. As soon as the IP phone requests a DHCP response, a rogue DHCP server can initiate a response with data fields containing false information.

This attack allows for possible man in the middle attacks on the IP-media gateway, and IP Phones. Many methods exist with the potential to reboot the phone remotely, e.g. “social engineering”, ping flood, MAC spoofing (probably SNMP hooks, etc.).

REMEDIATION: If possible, use static IP addresses for the IP Phones. This will remove the necessity of using a DHCP server. Further, using a state based intrusion detection system can filter out DHCP server packets from IP Phone ports, allowing this traffic only from the legitimate server.

TFTP Server Insertion Attack

It is possible to change the configuration of a target phone by exploiting the TFTP response race when the IP phone is resetting. A rogue TFTP server can supply spurious information before the legitimate server is able to respond to a request. This attack allows an attacker to change the configuration of an IP Phone.

REMEDIATION: Using a state based intrusion detection system can filter out DHCP server packets from IP Phone ports, allowing such traffic only from the legitimate server. Organizations looking to deploy VoIP systems should look for IP Phone instruments that can download signed binary files.

Availability and Denial of Service

Availability refers to the notion that information and services be available for use when needed. Availability is the most obvious risk for a switch. Attacks exploiting vulnerabilities in the switch software or protocols may lead to deterioration or even denial of service or functionality of the switch. For example: if unauthorized access can be established to any branch of the communication channel (such as a CCS link or a TCP/IP link), it may be possible to flood the link with bogus messages causing severe deterioration (possibly denial) of service. A voice over IP system may have additional vulnerabilities with Internet connections. Because intrusion detection systems fail to intercept a significant percentage of Internet based attacks, attackers may be able to bring down VoIP systems by exploiting weaknesses in Internet protocols and services.

Any network may be vulnerable to denial of service attacks, simply by overloading the capacity of the system. With VoIP the problem may be especially severe, because of its sensitivity to packet loss or delay.

CPU Resource Consumption Attack without any account information.

An attacker with remote terminal access to the server may be able to force a system restart (shutdown all/restart all) by providing the maximum number of characters for the login and password buffers multiple times in succession. Additionally, IP Phones may reboot as a result of this attack.

In addition to producing a system outage, the restart may not restore uncommitted changes or, in some cases, may restore default passwords, which would introduce intrusion vulnerabilities.

REMEDIATION: The deployment of a firewall disallowing connections from unnecessary or unknown network entities is the first step to overcoming this problem. However, there is still the opportunity for an attacker to spoof his MAC and IP address, circumventing the firewall protection.

Default Password Vulnerability

It is common for switches to have a default login/password set, e.g., admin/admin, or root /root. Similarly, VoIP telephones often have default keypad sequences that can be used to unlock and modify network information

This vulnerability would allow an attacker to control the topology of the network remotely, allowing for not only complete denial of service to the network, but also a port mirroring attack to the attacker's location, giving the ability to intercept any other conversations taking place over the same switch. Further, the switch may have a web server interface, providing an attacker with the ability to disrupt the network without advance knowledge of switch operations and commands. In most systems, telephones download their configuration data on startup using TFTP or similar protocols. The configuration specifies the IP addresses for Call Manager nodes, so an attacker could substitute another IP address pointing to a call manager that would allow eavesdropping or traffic analysis.

REMEDIATION: Changing the default password is crucial. Moreover, the graphical user interface should be disabled to prevent the interception of plaintext administration sessions.

Exploitable software flaws

Like other types of software, VoIP systems have been found to have vulnerabilities due to buffer overflows and improper packet header handling. These flaws typically occur because the software is not validating critical information properly. For example, a short integer may be used as a table index without checking whether the parameter passed to the function exceeds 32,767, resulting in invalid memory accesses or crashing of the system.

Exploitable software flaws typically result in two types of vulnerabilities: denial of service or revelation of critical system parameters. Denial of service can often be implemented remotely, by passing packets with specially constructed headers that cause the software to fail. In some cases the system can be crashed, producing a memory dump in which an intruder can find IP addresses of critical system nodes, passwords, or other security-relevant information. In addition, buffer overflows that allow the introduction of malicious code have been found in VoIP software, as in other applications.

REMEDIATION: These problems require action from the software vendor, and distribution of patches to administrators. Intruders monitor announcements of vulnerabilities, knowing that many organizations require days or weeks to update their software. Regular checking for software updates and patches is essential to reducing these vulnerabilities. Automated patch handling can assist in reducing the window of opportunity for intruders to exploit known software vulnerabilities.

Account Lockout Vulnerability

An attacker will be able to provide several incorrect login attempts at the telnet prompt until the account becomes locked out. (This problem is common to most password-protected systems, because it prevents attackers from repeating login attempts until the correct password is found by trying all possible combinations.)

The account is unable to connect to the machine for the set lockout time.

REMEDICATION: If remote access is not available, this problem can be solved with physical access control.

NIST Recommendations.

Because of the integration of voice and data in a single network, establishing a secure VoIP and data network is a complex process that requires greater effort than that required for data-only networks. In particular, start with these general guidelines, recognizing that practical considerations, such as cost or legal requirements, may require adjustments for the organization:

1. Develop appropriate network architecture.

- Separate voice and data on logically different networks if feasible. Different subnets with separate RFC 1918 address blocks should be used for voice and data traffic, with separate DHCP servers for each, to ease the incorporation of intrusion detection and VoIP firewall protection at the voice gateway, which interfaces with the PSTN, disallow H.323, SIP, or other VoIP protocols from the data network. Use strong authentication and access control on the voice gateway system, as with any other critical network component. Strong authentication of clients towards a gateway often presents difficulties, particularly in key management. Here, access control mechanisms and policy enforcement may help.
- A mechanism to allow VoIP traffic through firewalls is required. There are a variety of protocol dependent and independent solutions, including application level gateways (ALGs) for VoIP protocols, Session Border Controllers, or other standards-based solutions when they mature.
- Stateful packet filters can track the state of connections, denying packets that are not part of a properly originated call. (This may not be practical when multimedia protocol inherent security or lower layer security is applied, e.g., H.235 Annex D for integrity provision or TLS to protect SIP signaling.)
- Use IPsec or Secure Shell (SSH) for all remote management and auditing access. If practical, avoid using remote management at all and do IP PBX access from a physically secure system.
- If performance is a problem, use encryption at the router or other gateway, not the individual endpoints, to provide for IPsec tunneling. Since some VoIP endpoints are not computationally powerful enough to perform encryption, placing this burden at a central point ensures all VoIP traffic emanating from the enterprise network has been encrypted. Newer IP phones are able to provide Advanced Encryption System (AES) encryption at reasonable cost. Note that Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules, is applicable to all Federal agencies that use

cryptographic-based security systems to protect sensitive information in computer and telecommunication systems (including voice systems) as defined in Section 5131 of the Information Technology Management Reform Act of 1996, Public Law 104-106.

2. Ensure that the organization has examined and can acceptably manage and mitigate the risks to their information, system operations, and continuity of essential operations when deploying VoIP systems.

VoIP can provide more flexible service at lower cost, but there are significant tradeoffs that must be considered. VoIP systems can be expected to be more vulnerable than conventional telephone systems, in part because they are tied in to the data network, resulting in additional security weaknesses and avenues of attack (see VoIP Risks, Threats, and Vulnerabilities section for more detailed discussion of vulnerabilities of VoIP and their relation to data network vulnerabilities).

Confidentiality and privacy may be at greater risk in VoIP systems unless strong controls are implemented and maintained. An additional concern is the relative instability of VoIP technology compared with established telephony systems. Today, VoIP systems are still maturing and dominant standards have not emerged. This instability is compounded by VoIP's reliance on packet networks as a transport medium. The public switched telephone network is ultra-reliable. Internet service is generally much less reliable, and VoIP cannot function without Internet connections, except in the case of large corporate or other users who may operate a private network. Essential telephone services, unless carefully planned, deployed, and maintained, will be at greater risk if based on VoIP.

3. Special consideration should be given to E-911 emergency services communications, because E-911 automatic location service is not available with VoIP in some cases.

Unlike traditional telephone connections, which are tied to a physical location, VoIP's packet switched technology allows a particular number to be anywhere. This is convenient for users, because calls can be automatically forwarded to their locations. But the tradeoff is that this flexibility severely complicates the provision of E-911 service, which normally provides the caller's location to the 911 dispatch office. Although most VoIP vendors have workable solutions for E-911 service, government regulators and vendors are still working out standards and procedures for 911 services in a VoIP environment. Agencies must carefully evaluate E-911 issues in planning for VoIP deployment.

4. Agencies should be aware that physical controls are especially important in a VoIP environment and deploy them accordingly.

Unless the VoIP network is encrypted, anyone with physical access to the office LAN could potentially connect network monitoring tools and tap into telephone conversations. Although conventional telephone lines can also be monitored when physical access is obtained, in most offices there are many more points to connect with a LAN without arousing suspicion. Even if encryption is used, physical access to VoIP servers and gateways may allow an attacker to do traffic analysis (i.e., determine which parties are communicating). Agencies therefore should ensure that adequate physical security is in place to restrict access to VoIP network components. Physical securities measures,

including barriers, locks, access control systems, and guards, are the first line of defense. Agencies must make sure that the proper physical countermeasures are in place to mitigate some of the biggest risks such as insertion of sniffers or other network monitoring devices. Otherwise, practically speaking this means that installation of a sniffer could result in not just data but all voice communications being intercepted.

5. VoIP-ready firewalls and other appropriate protection mechanisms should be employed. Agencies must enable, use, and routinely test the security features that are included in VoIP systems.

Because of the inherent vulnerabilities (e.g. susceptibility to packet sniffing) when operating telephony across a packet network, VoIP systems incorporate an array of security features and protocols. Organization security policy should ensure that these features are used. In particular, firewalls designed for VoIP protocols are an essential component of a secure VoIP system.

6. If practical, “softphone” systems, which implement VoIP using an ordinary PC with a headset and special software, should not be used where security or privacy are a concern.

Worms, viruses, and other malicious software are extraordinarily common on PCs connected to the internet, and very difficult to defend against. Well-known vulnerabilities in web browsers make it possible for attackers to download malicious software without a user’s knowledge, even if the user does nothing more than visit a compromised web site. Malicious software attached to email messages can also be installed without the user’s knowledge, in some cases even if the user does not open the attachment. These vulnerabilities result in unacceptably high risks in the use of “softphones”, for most applications. In addition, because PCs are necessarily on the data network, using a softphone system conflicts with the need to separate voice and data networks to the greatest extent practical.

7. If mobile units are to be integrated with the VoIP system, use products implementing WiFi Protected Access (WPA), rather than 802.11 Wired Equivalent Privacy (WEP).

The security features of 802.11 WEP provide little or no protection because WEP can be cracked with publicly available software. The more recent WiFi Protected Access (WPA), a snapshot of the ongoing 802.11i standard, offers significant improvements in security, and can aid the integration of wireless technology with VoIP. NIST strongly recommends that the WPA (or WEP if WPA is unavailable) security features be used as part of an overall defense-in-depth strategy. Despite their weaknesses, the 802.11 security mechanisms can provide a degree of protection against unauthorized disclosure, unauthorized network access, or other active probing attacks. However, the Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules, is mandatory and binding for Federal agencies that have determined that certain information must be protected via cryptographic means. As currently defined, neither WEP nor WPA meets the FIPS 140-2 standard. In these cases, it will be necessary to employ higher level cryptographic protocols and applications such as secure shell (SSH), Transport Level Security (TLS) or Internet Protocol Security (IPsec) with FIPS 140-2 validated cryptographic modules and associated algorithms to protect information, regardless of whether the nonvalidated data link security protocols are used.

8. Carefully review statutory requirements regarding privacy and record retention with competent legal advisors.

Although legal issues regarding VoIP are beyond the scope of this document, readers should be aware that laws and rulings governing interception or monitoring of VoIP lines, and retention of call records, may be different from those for conventional telephone systems. Agencies should review these issues with their legal advisors. See Section 2.5 for more on these issues.

G.3 Cloud Computing White Paper

Cloud Computing

Purpose:

This paper is provided to define and describe cloud computing, discuss CJIS Security Policy (CSP) compliance, detail security and privacy, and provide general recommendations.

Attribution:

- NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing (Dec. 2011)
- NIST SP 800-145, the NIST Definition of Cloud Computing (Sept. 2011)
- NIST SP 800-146, Cloud Computing Synopsis and Recommendations (May 2011)
- CJIS Security Policy, Version 5.0

Definitions and Terms:

Cloud computing – A distributed computing model that permits on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services), software, and information.

Cloud subscriber – A person or organization that is a customer of a cloud

Cloud client – A machine or software application that accesses a cloud over a network connection, perhaps on behalf of a subscriber

Cloud provider – An organization that provides cloud services

Summary:

With many law enforcement agencies looking for ways to attain greater efficiency while grappling with reduced budgets, the idea of cloud computing to maintain data and applications is a viable business solution. But the unique security and legal characteristics of law enforcement agencies means any migration to cloud services may be challenging. Anytime the security of information and transactions must be maintained, as it must be with access to the FBI's CJIS systems and the protection of Criminal Justice Information (CJI), security and policy compliance concerns are bound to arise.

Cloud computing has become a popular and sometimes contentious topic of discussion for both the private and public sectors. This is in part because of the difficulty in describing cloud computing in general terms, because it is not a single kind of system. The “cloud” spans a spectrum of underlying technologies, configuration possibilities, service and deployment models. Cloud computing offers the ability to conveniently rent access to fully featured applications, software development and deployment environments, and computing infrastructure assets - such as network-accessible data storage and processing from a cloud service provider.

Ultimately, the move to cloud computing is a business decision in which the following relevant factors are giving proper consideration:

- readiness of existing applications for cloud deployment
- transition costs
- life-cycle costs
- maturity of service orientation in existing infrastructure
- security and privacy requirements – federal, state, and local

Achieving CJIS Security Policy Compliance:

The question that is often asked is, “Can an Agency be compliant with the CSP and also cloud compute?”

Because the CSP is device and architecture independent (per CSP Section 2.2), the answer is yes, and this can be accomplished— assuming the vendor of the cloud technology is able to meet the existing requirements of the CSP.

There are security challenges that must be addressed if CJI is to be sent into or through, stored within, or accessed from the cloud.

Admittedly, the existing CSP requirements may be difficult for some cloud-computing vendors due to the sheer numbers and the geographic disbursement of their personnel; however, the requirements aren’t new to vendors serving the criminal justice community and many vendors have been successfully meeting the CSP requirements for years. Even so, they are the minimum security requirements which will provide an acceptable level of assurance that law enforcement and personally identifiable information (PII) will be protected when shared with other law enforcement agencies across the nation.

Before tackling these challenges, the cloud subscriber should first be aware of what security and legal requirements they are subject to prior to entering into any agreement with a cloud provider. The following questions can help frame the process of determining compliance with the existing requirements of the CSP.

- Will access to Criminal Justice Information (CJI) within a cloud environment fall within the category of remote access? (5.5.6 Remote Access)
- Will advanced authentication (AA) be required for access to CJI within a cloud environment? (5.6.2.2 Advanced Authentication, 5.6.2.2.1 Advanced Authentication Policy and Rationale)
- Does/do any cloud service provider's datacenter(s) used in the transmission or storage of CJI meet all the requirements of a physically secure location? (5.9.1 Physically Secure Location)
- Are the encryption requirements being met? (5.10.1.2 Encryption)
 - Who will be providing the encryption as required in the CJIS Security Policy? (client or cloud service provider)
 - Is the data encrypted while at rest and in transit?
- What are the cloud service provider's incident response procedures? (5.3 Policy Area 3: Incident Response)
 - Will the cloud subscriber be notified of any incident?
 - If CJI is compromised, what are the notification and response procedures?
- Is the cloud service provider a private contractor/vendor?
 - If so, they are subject to the same screening and agreement requirements as any other private contractors hired to handle CJI? (5.1.1.5 Private Contractor User Agreements and CJIS Security Addendum; 5.12.1.2 Personnel Screening for Contractors and Vendors)
- Will the cloud service provider allow the CSA and FBI to conduct compliance and security audits? (5.11.1 Audits by the FBI CJIS Division; 5.11.2 Audits by the CSA)
- How will event and content logging be handled? (5.4 Policy Area 4, Auditing and Accountability)
 - Will the cloud service provider handle logging and provide that upon request?

Ultimately, the goal is to remain committed to using technology in its information sharing processes, but not at the sacrifice of the security of the information with which it has been entrusted. As stated in the CSP, device and architecture independence can permit the use of cloud computing, but the security requirements do not change.

The Cloud Model Explained:

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

The cloud model as defined by NIST consists of five essential characteristics, offers the option of three service models, and may be deployed via any of four deployment models as shown in Figure 1 below:

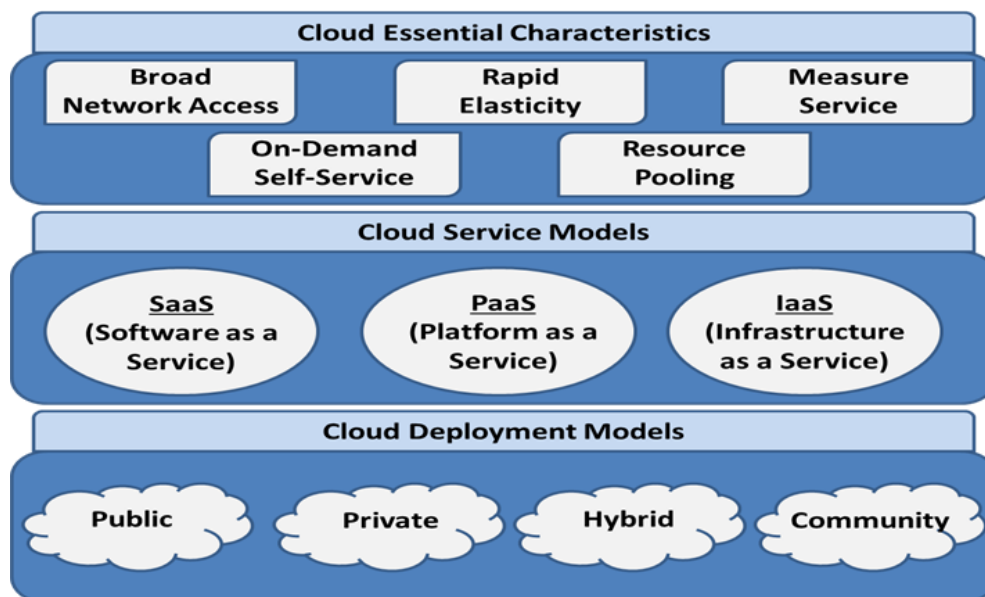


Figure 1 - Visual Depiction of the NIST Cloud Computing Definition

Essential Characteristics:

On-demand self-service

A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Broad network access

Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling

The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

Rapid elasticity

Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

Measured service

Cloud systems automatically control and optimize resource use by leveraging a metering capability* at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

** Typically this is done on a pay-per-use or charge-per-use basis.*

Deployment Models:

Private cloud

The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Community cloud

The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Public cloud

The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Hybrid cloud

The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

Service Models:

Software as a Service (SaaS)

This model provides the consumer the capability to use the provider's applications running on a cloud infrastructure*.

** A cloud infrastructure is the collection of hardware and software that enables the five essential characteristics of cloud computing. The cloud infrastructure can be viewed as containing both a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are necessary to support the cloud services being provided, and typically includes server, storage and network components. The abstraction layer consists of the software deployed across the physical layer, which manifests the essential cloud characteristics. Conceptually the abstraction layer sits above the physical layer.*

The SaaS service model is often referred to as "Software deployed as a hosted service and accessed over the Internet."

The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface.

When using the SaaS service model it should be understood that the consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Platform as a Service (PaaS)

This model provides the consumer the capability to deploy consumer-created or acquired applications* created using programming languages, libraries, services, and tools supported by the provider onto the cloud infrastructure.

** This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources.*

When using the PaaS service model the consumer may have control over the deployed applications and possibly configuration settings for the application-hosting environment, but does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage.

Infrastructure as a Service (IaaS)

This model provides the consumer the capability to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.

When using the IaaS service model the consumer may have control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls), but does not manage or control the underlying cloud infrastructure.

Key Security and Privacy Issues:

Although the emergence of cloud computing is a recent development, insights into critical aspects of security can be gleaned from reported experiences of early adopters and also from researchers analyzing and experimenting with available cloud provider platforms and associated technologies. The sections below highlight privacy and security-related issues that are believed to have long-term significance for public cloud computing and, in many cases, for other cloud computing service models.

Because cloud computing has grown out of an amalgamation of technologies, including service oriented architecture, virtualization, Web 2.0, and utility computing, many of the privacy and security issues involved can be viewed as known problems cast in a new setting. The importance of their combined effect in this setting, however, should not be discounted. Public cloud computing does represent a thought-provoking paradigm shift from conventional norms to an open organizational infrastructure—at the extreme, *displacing applications from one organization's infrastructure to the infrastructure of another organization, where the applications of potential adversaries may also operate.*

Governance

Governance implies control and oversight by the organization over policies, procedures, and standards for application development and information technology service acquisition, as well as the design, implementation, testing, use, and monitoring of deployed or engaged services. With the wide availability of cloud computing services, lack of organizational controls over employees engaging such services arbitrarily can be a source of problems. While cloud computing simplifies platform acquisition, it doesn't alleviate the need for governance; instead, it has the opposite effect, amplifying that need.

Dealing with cloud services requires attention to the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met. Ensuring systems are secure and risk is managed is challenging in any environment and even more daunting with cloud computing. Audit mechanisms and tools should be in place to determine how data is stored, protected, and used, to validate services, and to verify policy enforcement. A risk management program should also be in place that is flexible enough to deal with the continuously evolving and shifting risk landscape.

Compliance

Compliance refers to an organization's responsibility to operate in agreement with established laws, regulations, standards, and specifications. Various types of security and privacy laws and regulations exist within different countries at the national, state, and local levels, making compliance a potentially complicated issue for cloud computing.

Law and Regulations

Cloud providers are becoming more sensitive to legal and regulatory concerns, and may be willing to commit to store and process data in specific jurisdictions and apply required safeguards for security and privacy. However, the degree to which they will accept liability in their service agreements, for exposure of content under their control, remains to be seen. Even so, organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf.

Data Location

One of the most common compliance issues facing an organization is data location. A characteristic of many cloud computing services is that data is stored redundantly in multiple physical locations and detailed information about the location of an organization's data is unavailable or not disclosed to the service consumer. This situation makes it difficult to ascertain whether sufficient safeguards are in place and whether legal and regulatory compliance requirements are being met. External audits and security certifications can alleviate this issue to some extent, but they are not a panacea.

When information crosses borders, the governing legal, privacy, and regulatory regimes can be ambiguous and raise a variety of concerns. Consequently, constraints on the trans-border flow of sensitive data, as well as the requirements on the protection afforded the data, have become the subject of national and regional privacy and security laws and regulations.

Electronic Discovery

The capabilities and processes of a cloud provider, such as the form in which data is maintained and the electronic discovery-related tools available, affect the ability of the organization to meet its obligations in a cost effective, timely, and compliant manner. A cloud provider's archival capabilities may not preserve the original metadata as expected, causing spoliation (i.e., the intentional, reckless, or negligent destruction, loss, material alteration, or obstruction of evidence that is relevant to litigation), which could negatively impact litigation.

Trust

Under the cloud computing paradigm, an organization relinquishes direct control over many aspects of security and privacy, and in doing so, confers a high level of trust onto the cloud provider. At the same time, federal agencies have a responsibility to protect information and information systems commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction, regardless of whether the information is collected or maintained by or on behalf of the agency; or whether the information systems are used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency

Insider Access

Data processed or stored outside the physical confines of an organization, its firewall, and other security controls bring with it an inherent level of risk. The insider security threat is a well-known issue for most organizations. Incidents may involve various types of fraud, sabotage of information resources, and theft of sensitive information.

Data Ownership

The organization's ownership rights over the data must be firmly established in the service contract to enable a basis for trust and privacy of data. The continuing controversy over privacy and data ownership rights for social networking users illustrates the impact that ambiguous terms can have on the parties involved.

Ideally, the contract should state clearly that the organization retains exclusive ownership over all its data; that the cloud provider acquires no rights or licenses through the agreement, including intellectual property rights or licenses, to use the organization's data for its own purposes; and that the cloud provider does not acquire and may not claim any interest in the data due to security. For these provisions to work as intended, the terms of data ownership must not be subject to unilateral amendment by the cloud provider.

Visibility

Continuous monitoring of information security requires maintaining ongoing awareness of security controls, vulnerabilities, and threats to support risk management decisions. Transition to public cloud services entails a transfer of responsibility to the cloud provider for securing portions of the system on which the organization's data and applications operate.

Ancillary Data

While the focus of attention in cloud computing is mainly on protecting application data, cloud providers also hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks.

Risk Management

Assessing and managing risk in systems that use cloud services can be a challenge. With cloud-based services, some subsystems or subsystem components fall outside of the direct control of a client organization. Many organizations are more comfortable with risk when they have greater control over the processes and equipment involved. Establishing a level of trust about a cloud service is dependent on the degree of control an organization is able to exert on the provider to provision the security controls necessary to protect the organization's data and applications, and also the evidence provided about the effectiveness of those controls. Ultimately, if the level of trust in the service falls below expectations and the organization is unable to employ compensating controls, it must either reject the service or accept a greater degree of risk.

Architecture

The architecture of the software and hardware used to deliver cloud services can vary significantly among public cloud providers for any specific service model. It is important to understand the technologies the cloud provider uses to provision services and the implications the technical controls involved have on security and privacy of the system throughout its lifecycle. With such information, the underlying system architecture of a cloud can be decomposed and mapped to a framework of security and privacy controls that can be used to assess and manage risk.

Identity and Access Management

Data sensitivity and privacy of information have become increasingly an area of concern for organizations. The identity proofing and authentication aspects of identity management entail the use, maintenance, and protection of PII collected from users. Preventing unauthorized access to information resources in the cloud is also a major consideration. One recurring issue is that the

organizational identification and authentication framework may not naturally extend into a public cloud and extending or changing the existing framework to support cloud services may prove difficult.

Software Isolation

High degrees of multi-tenancy over large numbers of platforms are needed for cloud computing to achieve the envisioned flexibility of on-demand provisioning of reliable services and the cost benefits and efficiencies due to economies of scale. Regardless of the service model and multi-tenant software architecture used, the computations of different consumers must be able to be carried out in isolation from one another, mainly through the use of logical separation mechanisms.

Data Protection

Data stored in a public cloud typically resides in a shared environment collocated with data from other customers. Organizations placing sensitive and regulated data into a public cloud, therefore, must account for the means by which access to the data is controlled and the data is kept secure. Similar concerns exist for data migrated within or between clouds.

Value Concentration

Having data collocated with that of an organization with a high threat profile could also lead to a denial of service, as an unintended casualty from an attack targeted against that organization. Similarly, side effects from a physical attack against a high profile organization's cloud-based resources are also a possibility. For example, over the years, facilities of the Internal Revenue Service have attracted their share of attention from would-be attackers.

Data Isolation

Database environments used in cloud computing can vary significantly. Accordingly, various types of multi-tenant arrangements exist for databases. Each arrangement pools resources differently, offering different degrees of isolation and resource efficiency. Regardless of implementation decision, data must be secured while at rest, in transit, and in use, and access to the data must be controlled.

Data Sanitization

The data sanitization practices that a cloud provider implements have obvious implications for security. Sanitization involves the expunging of data from storage media by overwriting, degaussing, or other means, or the destruction of the media itself, to

prevent unauthorized disclosure of information. Data sanitization also applies to backup copies made for recovery and restoration of service and residual data remaining upon termination of service.

In a public cloud computing environment, data from one consumer is physically collocated (e.g., in an IaaS data store) or commingled (e.g., in a SaaS database) with the data of other consumers, which can complicate matters. Service agreements should stipulate sufficient measures that are taken to ensure data sanitization is performed appropriately throughout the system lifecycle.

Encryption

Client end-to-end encryption (e.g. encryption/decryption occurs on the law enforcement controlled client prior to data entering the cloud and decryption occurs only on the client device after encrypted data is removed from the cloud service) with cryptographic keys managed solely by law enforcement would prevent exposure of sensitive data.

- May cause significant cloud service functionality limitations on available service types made available for sensitive data. This may also increase expenses to cover key items, such as key management and client software. Additionally, a number of specific SLA or contract clauses may be necessary for the implementation of client end-to end encryption.

Use of cloud services without end-to-end encryption implemented by the client is another option that would require cloud service provider participation in the encryption of data.

- This would require at least some cloud provider personnel to undergo personnel background screening and training.
- Specialized Service Level Agreements (SLA) and/or contractual clauses would be necessary to identify those personnel that may have access to unencrypted, sensitive data.
- Conducting the analysis and gaining approval of particular cloud service implementations not utilizing end-to-end encryption for sensitive law enforcement data may be costly and time consuming due to the high degree of technical complexity.

Availability

In simple terms, availability is the extent to which an organization's full set of computational resources is accessible and usable. Denial of service attacks, equipment outages, and natural disasters are all threats to availability. The concern is that most downtime is unplanned and can

impact the mission of the organization. Some examples of unplanned service interruptions that cause concerns are:

- Temporary Outages
- Prolonged and Permanent Outages
- Denial of Service

Incident Response

The complexity of a cloud service can obscure recognition and analysis of incidents. Revising an organization's incident response plan to address differences between the organizational computing environment and a cloud computing environment is an important, but easy-to-overlook prerequisite to transitioning applications and data.

Data Availability

The availability of relevant data from event monitoring is essential for timely detection of security incidents. Cloud consumers are often confronted with extremely limited capabilities for detection of incidents in public cloud environments. The situation varies among cloud service models and cloud providers. For example, PaaS providers typically do not make event logs available to consumers, who are then left mainly with event data from self-deployed applications (e.g., via application logging). Similarly, SaaS consumers are completely dependent upon the cloud provider to provide event data such as activity logging, while IaaS consumers control more of the information stack and have access to associated event sources.

Incident Analysis and Resolution

An analysis to confirm the occurrence of an incident or determine the method of exploit needs to be performed quickly and with sufficient detail of documentation and care to ensure that traceability and integrity is maintained for subsequent use, if needed (e.g., a forensic copy of incident data for legal proceedings). Issues faced by cloud consumers when performing incident analysis include lack of detailed information about the architecture of the cloud relevant to an incident, lack of information about relevant event and data sources held by the cloud provider, ill-defined or vague incident handling responsibilities stipulated for the cloud provider, and limited capabilities for gathering and preserving pertinent data sources as evidence. Understanding and negotiating the provisions and procedures for incident response should be done before entering into a service contract, rather than as an afterthought.

General Recommendations:

A number of significant security and privacy issues were covered in the previous subsections. Table 1 summarizes those issues and related recommendations for organizations to follow when planning, reviewing, negotiating, or initiating a public cloud service outsourcing arrangement.

Table 1: Security and Privacy Issue Areas and Recommendations

Areas	Recommendations
Governance	• Extend organizational practices pertaining to the policies, procedures, and standards used for application development and service provisioning in the cloud, as well as the design, implementation, testing, use, and monitoring of deployed or engaged services. • Put in place audit mechanisms and tools to ensure organizational practices are followed throughout the system lifecycle.
Compliance	• Understand the various types of laws and regulations that impose security and privacy obligations on the organization and potentially impact cloud computing initiatives, particularly those involving data location, privacy and security controls, records management, and electronic discovery requirements. • Review and assess the cloud provider's offerings with respect to the organizational requirements to be met and ensure that the contract terms adequately meet the requirements. • Ensure that the cloud provider's electronic discovery capabilities and processes do not compromise the privacy or security of data and applications.
Trust	• Ensure that service arrangements have sufficient means to allow visibility into the security and privacy controls and processes employed by the cloud provider, and their performance over time. • Establish clear, exclusive ownership rights over data. • Institute a risk management program that is flexible enough to adapt to the constantly evolving and shifting risk landscape for the lifecycle of the system. • Continuously monitor the security state of the information system to support on-going risk management decisions.
Architecture	• Understand the underlying technologies that the cloud provider uses to provision services, including the implications that the technical controls involved have on the security and privacy of the system, over the full system lifecycle and across all system components.
Identity and Access Management	• Ensure that adequate safeguards are in place to secure authentication, authorization, and other identity and access management functions, and are suitable for the organization.

Software Isolation	• Understand virtualization and other logical isolation techniques that the cloud provider employs in its multi-tenant software architecture, and assess the risks involved for the organization.
Data Protection	• Evaluate the suitability of the cloud provider's data management solutions for the organizational data concerned and the ability to control access to data, to secure data while at rest, in transit, and in use, and to sanitize data. • Take into consideration the risk of collating organizational data with that of other organizations whose threat profiles are high or whose data collectively represent significant concentrated value. • Fully understand and weigh the risks involved in cryptographic key management with the facilities available in the cloud environment and the processes established by the cloud provider.
Availability	• Understand the contract provisions and procedures for availability, data backup and recovery, and disaster recovery, and ensure that they meet the organization's continuity and contingency planning requirements. • Ensure that during an intermediate or prolonged disruption or a serious disaster, critical operations can be immediately resumed, and that all operations can be eventually reinstituted in a timely and organized manner.
Incident Response	• Understand the contract provisions and procedures for incident response and ensure that they meet the requirements of the organization. • Ensure that the cloud provider has a transparent response process in place and sufficient mechanisms to share information during and after an incident. • Ensure that the organization can respond to incidents in a coordinated fashion with the cloud provider in accordance with their respective roles and responsibilities for the computing environment.

G.4 Mobile Appendix

Mobile Appendix

Introduction

Mobile devices present a unique security challenge with regard to the correct application of CJIS Security Policy requirements. This appendix is intended to provide best practices based on industry standards and on methods to achieve policy compliance in mobile device employment scenarios. The technical methods used to achieve compliance with CJIS Security Policy will typically be different within the mobile environment than those used in fixed locations. Many of the security features and capabilities inherited by endpoint devices from the fixed environment are either not present or present in a different form in the mobile environment. Additionally, the basic technologies used in some types of mobile devices may adequately fulfill some of the CJIS Security Policy requirements which would require additional software or added features in a traditional fixed computing environment. Due to the complexity and rapid evolution of the mobile environment, this Appendix will remain as device and vendor agnostic as practical, however certain key requirements for specific mobile operating systems will be identified for the major mobile operating systems (e.g. Apple iOS, Android) as the underlying technologies are fundamentally different and offer different levels of built-in compliance to CJIS Security Policy.

Sections within this appendix will provide recommendations regarding priorities and level of effort versus value of applying certain security controls in the mobile environment. These recommendations do not supersede or modify the requirements listed in the CJIS Security Policy, and are intended to describe the effect of inherent security functions and inherent device limitations in many mobile platforms that impact the application of policy elements in the mobile environment.

Mobile Device Risk Scenarios

There are multiple risk scenarios that may apply to mobile devices depending on the category of device (e.g. Laptop, Tablet, and 'Pocket sized' devices such as smartphones) and the methods of device connectivity (e.g. cellular service, WiFi + Cellular, WiFi only). Device category and method of connection define the technology types within the device which inherently affects the total level of compliance with CJIS Security Policy that can be obtained by the mobile device.

It is advisable for acquiring agencies to review the mobile device guidance in this Appendix prior to completing selection and acquisition of particular devices. Both the device category and connectivity methods installed and configured on the device will impact the overall risk scenario associated with the device and may significantly affect the effective cost to bring use of the device in compliance with the CJIS Security Policy. For instance, inclusion of cellular radios with the ability to remotely control a device significantly changes the risk scenario by allowing remote tracking, file deletion, and device management which could provide a higher level of CJIS Security Policy compliance than a WiFi only device that does not guarantee the ability to remotely manage the device. However, inclusion of cellular technology may significantly increase the initial device costs and incur ongoing subscription costs. Appropriate choices based on the intended use of the device along with the types and methods of Criminal Justice Information (CJI) data to be accessed could greatly reduce agency cost and enhance security.

Device Categories

This appendix defines risk levels for three categories of devices. Prior to reading individual sections of this Appendix, the agency should identify which device categories will apply to their employment scenario. If multiple categories of devices are employed, individual technical configurations and local policy will likely need to be defined for each category of device based on the risk inherent in the technical characteristics associated with each device category.

Laptop devices

The laptop device category includes mobile devices in a larger format that are transported either in a vehicle mount or a carrying case and include a monitor with attached keyboard. This includes all traditional laptop computers that utilize a 'traditional', full featured operating system (e.g. Windows or a Linux variant). Also included in this category are 'tablet' type full featured computers running a traditional full featured operating system but without an attached keyboard. The main defining factor is the use of a full featured operating system and a form factor to large to be carried in a pocket. In general, devices of this type connect via WiFi only, but may include an internal cellular access card in some cases.

The risks associated with this device type are similar to a standard desktop computer at the technical level, but are increased due to the potential to connect directly to the internet without the benefit of organizational network security layers (e.g. network firewall, IDS/IPS, network monitoring devices). There is also an increased risk of intentional device theft from vehicles or unsecure locations as these devices are too large to be carried on the authorized user's body. There may be increased risk from the limited technical ability to wipe or track a lost/stolen device depending on the particular technical means used for remote device connectivity (e.g. cellular or WiFi).

In general, the technical configurations for compliance with most of the CJIS Security Policy that is accomplished via the operating system (e.g. auditing, access control, etc) will remain consistent with normal fixed location computing systems for laptop devices, but some functions may operate in an unexpected manner due to lack of constant connectivity. Thorough testing of applied security policy elements within the expected mobile environments will help ensure the applied policy configurations remain effective and appropriate when applied to mobile laptop devices.

NOTE: Some newer devices running multi-function operating systems (e.g. Windows 8 or similar multi-mode operating systems) may exhibit technical features associated with both laptop and tablet device categories based on their current operating mode which may be reconfigured by the user on demand. If this is the case, it will be necessary to assess and configure multiple operating modes to be compliant with CJIS Security Policy on the device, or restrict the operating mode to one category of operation.

Tablet devices

The tablet device category includes larger format devices transported via vehicle mount or portfolio sized carry case that typically consist of a touch screen without attached keyboard. These devices utilize a limited feature operating system (e.g. Apple iOS, Google Android, Windows mobile) that is inherently more resistant than a traditional operating system to certain types of network based technical attacks due to the limited feature sets. Additionally, limited functionality operating systems are designed specifically for the mobile environment where

battery life and power efficiency are primary design drivers. This inherently limits the types of services that can function effectively on the devices (e.g. traditional real-time anti-virus software) as the base operating system may not be designed to allow installed applications enhanced execution priority in the background and or the ability to examine the contents or communications associated within another application. However, this same design methodology significantly limits the vectors available for malware transmission and the device or application data actually accessible to malware if a device becomes infected.

Tablet devices will have different risks associated depending on the installed and configured methods for network access (e.g. ‘always on cellular’ vs. WiFi only). Physical risks associated with this category are similar to the laptop category for enhanced likelihood of intentional theft or device hijacking while unattended, while the technical risks are similar to the pocket device category.

Pocket devices/Handheld devices

The pocket/handheld device category is technically similar or identical to the tablet category and is primarily differentiated by device form factor. Pocket/handheld devices are characterized as having a limited functionality operating system and a small form factor intended for carry in a pocket or ‘holster’ attached to the body. The bulk of this category will be cellular ‘smartphones’ with integrated cellular data connectivity, however devices intended to be worn or carried on the body (e.g. portable fingerprint devices) may also be included in this category if they operate using a limited functionality operating system. Custom or specialty devices may meet the form factor distinction for this category, but operate using a full feature operating system. In rare cases of this nature the employing agency should apply security guidance and principles in this appendix for both the laptop and pocket device categories.

Risks associated with this category are a reduced threat of theft to a stored devices (e.g. device left unattended in a vehicle) since these devices are typically carried continuously by the authorized user, but include a greater risk of temporary or permanent loss of control due to the device being misplaced by the authorized user.

Due to the installation of a limited functionality operating system, the technical threat to these devices via a network based attack is significantly lower than the laptop category, however, the threat of unauthorized access at the device level may be higher if the device is lost due to technical limits on multi-factor authentication to the operating system itself and practical limits to device passwords due to screen/software keyboard limitations.

NOTE: Data accessible on pocket or tablet devices simply through the entry of a single device PIN or password should not be considered secure due to the likelihood of enhanced password guessing based on fingerprints/smudges on the device touch screen. Any data stored on devices of these types should be protected within a separate secure container using Advanced Authentication.

Device Connectivity

There are three main categories of device connectivity that are associated with varying risk levels and threats to the devices. The Three categories are: Cellular Network Only (always on), WiFi Only (includes ‘on demand’ cellular), and Cellular (always on) + WiFi network. The risks associated with connectivity categories are general risks and may apply differently to any particular device at different points in its usage or lifecycle. Particular device configurations

either through the operating system or a third-party mobile device management (MDM) system may be able to significantly control and define which particular connectivity risks may be associated with a particular device.

Cellular Network Only (always on)

Cellular network connectivity is characterized by ‘always on’ network connection through the device internal radio to a cellular network provider. There is a reasonable assurance that devices with ‘always on’ cellular can be tracked, managed, or wiped remotely if lost or stolen. This will significantly reduce risks associated with loss of the device and attempted illicit access to the device. One important consideration for this risk category is characterization of the device as ‘always on’ or ‘on demand’. In effect the difference is typically a configuration setting, which in some cases may be changeable by the user. In particular most cellular smart phones contain ‘airplane’ mode settings that disable all internal radios allowing a user authenticated to the device operating system via password or personal identification number (PIN) to disable the cellular system. Access to this functionality may be disabled through the use of some MDM systems which would necessitate a complete power down of the device while carried on aircraft. Additionally, someone illicitly obtaining a device with properly configured password requirements and screen lock timeouts would be unlikely to guess the device password before the device was reported stolen in order for them to disable the cellular connection and prevent tracking or a remote wipe of the device.

Cellular networks do not allow for the same level of exposure of individual devices to random access from the internet. This significantly reduces the potential network based attack vectors that might reach a cellular connected device. The risk scenario in most cases from a network based attack would be similar to a device protected behind rudimentary network defenses (e.g. standard firewall but NOT advanced intrusion detection/prevention) Cellular device communications cannot typically be accessed by other ‘eavesdropping’ devices physically close to them without significant specialized equipment and can be considered well protected against network attacks below the nation/state level of technical capability by the hosting technical infrastructure and technology inherent in the device. However, network based attacks that utilize connections initiated by the user device may still succeed over the cellular infrastructure. For this reason, the technical protections inherent in the cellular infrastructure provide limited protection against user/device initiated actions (e.g. web surfing on a cellular connected web browser). Therefore, the protections provided by always on cellular connections are primarily in the ability to remotely access the mobile device for tracking or data deletion in case of device loss or compromise, which combined with a limited functionality device operating system, the protections are generally equivalent to a ‘personal firewall’ if properly configured and supported by a well designed organizational infrastructure. However, that equivalency does not apply to full featured operating systems connected through cellular infrastructure.

NOTE: It should be noted that a technically capable, intentional, thief knowingly obtaining an ‘always on’ cellular device for the purpose of data theft can physically disable the radio by utilizing a Faraday cage or similar external electromagnetic shield device while attempting to guess the device password. While technically possible these methods require specialized equipment and high technical expertise and would be very unlikely to be employed except for specifically targeted attacks. When always on cellular connectivity is combined with a robust incident reporting process and user training for rapid response to device loss or theft, the associated risks can be minimized.

WiFi only (includes 'on-demand' cellular)

WiFi only devices do not include cellular radios or include cellular radio that must be manually activated or 'connected' to the cellular network. They connect to the network or internet through WiFi 'hotspots' or external access points or manually to cellular networks. Some MDM or device configurations may be able to limit the types and specific WiFi access points the device can connect to, which may change the risk scenario of the device to a similar risk scenario as the Cellular Network Only scenario. However, if mobile devices are permitted (through technical and or policy decisions) to connect to any WiFi access point designated by the device user, the overall device risk scenario is high and the device may be accessible to a large number of potential network based attack vectors. Unrestricted WiFi access is not recommended on any agency owned device, but must be assumed to exist on any personally owned device authorized to access CJI. Significant compensating controls may be needed to ensure devices accessing CJI over 'public' WiFi access points are not susceptible to communications network eavesdropping, credential hijacking or any of the various potential man-in-the-middle attacks possible through access point spoofing. The communications security risks can be significantly mitigated by mandatory device configurations (e.g. MDM based policy) that only allow devices to connect to cryptographically verified agency controlled WiFi access points.

WiFi only or devices with 'on-demand' cellular access (e.g. user or event driven cellular access initiated from the device and not from a centralized management location) are significantly more at risk from data loss subsequent to device loss or theft as there is no guarantee the tracking or remote wipe can be initiated once the device is out of agency control. This can be mitigated by utilizing tracking/anti-theft products that require a periodic network connection to authorize access and perform automated device locking ('bricking') or remote wipe if network connections are not made within a specified period. Software of this nature is generally available for full featured laptops but may not be available for limited feature mobile operating systems.

Cellular (always on) + WiFi Network

This is a hybrid scenario that has become typical with most 'smartphones'. These devices contain both the always on cellular connection, but may also be configured to access local WiFi networks for enhanced bandwidth. In considering devices with these technical characteristics, the theft/loss risks are similar to the cellular only scenario (due to tracking and remote access through the cellular connection), while the data and network based risks must be considered to be similar to the WiFi scenario unless the capability of the device to connect to WiFi networks is limited by technology or policy to agency owned WiFi Access Points configured in accordance with the CJIS Security Policy. Careful consideration must be made to the particular configurations, management systems, and human oriented operational policies based on the particular technical capabilities and configurations of these types of devices.

Incident Handling (CJIS Security Policy Section 5.3)

Additional or enhanced incident reporting and handling procedures will need to be developed to cover mobile device operating scenarios. Various exploits and methods to compromise mobile devices require either specialized equipment or lengthy operations to implement. Rapid response to mobile device related incidents can significantly mitigate the risks associated with illicit data access either on the device itself or within online data resources associated with the device through an application or specialized interface. However, parallel or special incident handling procedures with associated equipment or systems may need to be put in place to properly

respond to incidents involving mobile devices. This section lists three areas where enhanced incident handling and response processes may need to be implemented to ensure mobile device compliance to the incident handling policy in Section 5.3.

If personally owned devices are utilized within the environment in a Bring Your Own device (BYOD) scenario, specialized and costly incident handling procedures and processes may need to be developed to support compliance for those devices. The costs associated with enhanced incident handling procedures may need to be incorporated in the cost and risk based analysis to allow personally owned devices in the BYOD scenario, as the technical methods and risk to achieve compliance under BYOD scenarios may exceed any cost savings potentially achieved through BYOD.

Loss of device Control

Mobile device users should be trained and provided with explicit user actions in case positive control of a mobile device is lost for any period of time. Loss of positive control means the device is in the physical control of non-CJIS authorized individual or the device is left unattended in an unsecure location (e.g. counter of the coffee shop). Even if the device is recovered quickly there is significant risk that either the device settings could be tampered with or data on the device could be illicitly accessed. The level of detail and particular scenarios identified in the agency incident response plan should be consistent with the presence of persistent CJI on the device or the technical means used to access CJI from the device (e.g. ask the question: “Is it reasonable to assume CJI could be accessed”) as well as the degree of device configuration control exercised by the user from the device main login. At a minimum, special incident handling procedures should be developed for the following scenarios:

- Device known to be locked, control loss of minimal duration
- Device lock state unknown at time of control loss, duration of loss minimal
- Device lock state unknown at time of control loss, duration of loss extended
- Device known to be unlocked at time of control loss, duration of loss more than momentary.

NOTE: Organizations should define appropriate time value criteria based on the operational environment for the above scenarios. For instance, a ‘momentary’ loss of control might be considered a matter of seconds in a situation where no one could reasonably have accessed the device, while ‘minimal’ durations might include a few minutes of time and ‘extended’ periods would be any time longer than a few minutes.

Other scenarios should be addressed as appropriate to the intended device employment, with explicit user and organizational actions identified based on the device technologies and any organizational management capabilities.

Total Loss of device

Incident response scenarios for the total loss of the device should be developed based on the methods/storage of CJI on the device, the lock state of the device at time of loss (known locked, known unlocked, or unknown), and the technical methods available for remote tracking or wiping of the device. It is critical to implement incident handling procedures quickly in this case. Remote wipe functions can be implemented for always on cellular devices with a high potential for success that may include positive confirmation from the device that the wipe was completed.

However, for WiFi only and on demand cellular devices, incident handling procedures that lock the device out of accessing CJI may be necessary, while there would be no guarantee that any CJI stored on the device could not eventually be accessed. For this reason, CJI should not generally be stored directly on WiFi only or on-demand cellular devices unless an extremely robust anti-tamper system is in place on the device itself.

Potential device Compromise (software/application)

Incident response scenarios for potential device compromise through intentional or unintentional user action should be developed to ensure compliance with policy. This includes rooting, jailbreaking or malicious application installation on the device during a loss of device control scenario or inappropriate user action in the installation of applications to the device (compromise can occur from either intentional threat agent actions or accidental user actions). Triggers for this incident handling process may be driven from either user notification or electronic detection of device tampering from an audit or MDM compliance check.

Audit and Accountability (CJIS Security Policy Section 5.4)

The ability to implement some Audit and Accountability functions specified in the CJIS Security Policy on mobile devices with limited function operating systems (e.g. Android, Apple iOS) is not natively included within the operating system. Either additional device management systems, enterprise mobility management (EMM) or MDM, or auditing from systems accessed by the mobile device will be necessary to ensure appropriate levels of auditing exist.

Auditable Events (reference 5.4.1)

Some of the specific audit requirements in the CJIS Security Policy may not be technically relevant to the mobile operating system due to its internal functioning. To achieve compliance with the CJIS Security Policy it will be necessary in most cases to utilize some form of MDM or EMM system. Additional auditable events that compensate for the technical limitations of limited function mobile operating systems may be available through the use of MDM systems (e.g. association of event with global positioning system (GPS) location of the device). Specific auditable events of interest in the mobile environment will depend on the intended device usage, compartmentalization of data on the device, and options available with the specific technologies employed. For instance, item 2 in Section 5.4.1.1 indicates an auditable event includes attempts to modify elements of user account modification. Due to the limited internal functions of mobile operating systems, this event type is not relevant to the operating system itself as they are generally provisioned with only a single non-modifiable user account on the device. To achieve compliance in a scenario where CJI is stored or accessed from a secure application on the device, auditing of access to the secure application either through application design, or third party MDM capability may provide an acceptable compensating control. For compliance with the policy each auditable event and event content must be compared to the particular technologies and applications employed to determine if adequate compensating controls are being met for audit items that either do not apply to mobile technologies or cannot be implemented within the technology itself.

Alternative and compensating controls that provide detailed audit of access to CJI either on the mobile device itself or through a controlled application to a central server may provide equivalent auditing capability to the events specified in the policy. However, multiple auditing systems may be required to replicate the auditing provided at the operating system level by a full

function operating system. Therefore, the overall auditing design should take into account retrieval and consolidation of events or audit data from multiple auditing systems as appropriate to comply with policy.

Audit Event Collection

Mobile devices without an ‘always-on’ cellular connection may pose technical challenges to ensure any audit records collected and stored on the mobile device itself can be retrieved for review and analysis per the CJIS Security Policy. Alternatively systems which explicitly require a network connection to a central server to access data or decrypt on-device storage may provide acceptable audit event collection and reporting since there is a guarantee that network connections must be in place for CJI to be accessed. Careful consideration should be made regarding the accessibility of audit records when developing the mobile audit scheme.

Access Control (CJIS Policy Section 5.5)

Access control associated to limited functionality mobile operating systems will typically operate in a different manner than full function operating systems. For instance there is normally not a provision for multiple user accounts on many mobile operating systems which may mean the policy requirements for access control (e.g. regarding account management) would not be apply to the mobile operating system, but should rather be applied to a particular application, either stand-alone to the device or as part of a client server architecture. Application of access control policy identified in the CJIS Security Policy will often need to be applied to elements of the total system beyond the device operating system.

For example, CJI stored or accessed from a secure mobile application that requires connectivity to a CJIS authorized server architecture could potentially accomplish most or all of the access control policy elements based on user authorization via the secured application and be largely independent of the mobile operating system. Alternatively, if storing CJI in ‘general’ purpose data storage containers on a mobile device it may not be possible to achieve compliance with the CJIS Security Policy. Careful consideration and deliberate design of mobile applications or data storage will be required to achieve compliance on mobile devices.

Due to the inherent nature of limited function mobile operating systems, very tight access controls to specific data is actually implemented within the operating system. This effectively prevents applications from accessing or manipulating data associated with other applications to a very high degree of confidence as long as the device is not rooted or jailbroken. However, the device user is automatically granted access to all device data through the associated application unless the application itself has a secondary authentication and access control methodology. Additionally, since basic device functions (e.g. phone) are typically protected using the same password or PIN as the device level encryption, use of a weak PIN to allow easy access to basic device functions largely negates the value of the integrated device encryption.

If personally owned devices are utilized within the environment (BYOD scenario), specialized and costly access control methods may be required to reach compliance with CJIS Security Policy. The costs associated with enhanced access control procedures and technologies should be incorporated in the cost and risk based analysis to determine whether or not to allow personally BYOD, as the technical methods and compensating controls required for CJIS Security Policy compliance are likely to exceed any potential cost savings for implementing BYOD.

Device Control levels and access.

Limited function mobile operating systems are typically very constrained on the levels of access provided to the user. However, intentional user actions (e.g. installing an application and accepting inappropriate security access levels for that application) may bypass some of the built in security protections inherent in the limited functionality devices. Compliance with CJIS Security Policy may be difficult without the addition of strict device control policy. In a mixed environment (e.g. agency owned devices and BYOD), access control policy with BYOD systems may be impractical or impossible to fully implement.

Embedded passwords/login tied to device PIN.

Limited function mobile operating systems typically allow the association of multiple passwords and access credentials with particular applications. The system access provided by these embedded credentials will often be tied to the device password or PIN. An example would be access to device integrated email and calendar applications. Alternatively a ‘corporate’ email application may independently encrypt the data associated with the application and require a separate login from the device itself. Access to CJI utilizing only the device level password or PIN and device embedded credentials is not compliant with CJIS Security Policy unless protected with Advanced Authentication, which is not currently possible on most devices. Therefore, use of integrated device functions (e.g. built in email or chat) to store or transmit CJI would also not be compliant.

Access requirement specification

In general, due to weaknesses associated with password guessing based on analysis of fingerprints or swipes on the device touch screen, short (4-8 digit) device PIN numbers provide limited security to a determined password guessing attack. Conversely, utilization of a robust password at the device level may be inconsistent with quick access to basic device functions (e.g. phone). When developing specific CJIS compliant access control and authentication schemas a layered approach with the device PIN protecting only the basic device functions (e.g. phone, camera, non-secure applications) and a more robust password or multifactor authentication used to protect applications or data storage may achieve policy compliance where the device password/PIN would not. In a layered security deployment, careful attention must be placed on the capability to share data (e.g. cut and paste or screenshot functions) between secure applications with CJI or CJI access and basic device functions with limited security controls.

Special Login attempt limit

Depending on the access and authentication scheme applied to the mobile device, it may be appropriate to fully comply with the CJIS login attempt limits within a secure application or container and not solely at the device level. However, the device itself should have login attempt limits consistent with the risk associated to the data or configurations accessible on the device itself. Since mobile devices are inherently portable, and can easily be removed from a location. Brute force attempts to gain access to the system, especially when protected only by a short PIN, are likely to be successful given sufficient time. Special consideration should be made based on device connectivity methods (cellular, WiFi, etc) on the appropriate number of unsuccessful login attempts that will be allowed and the resultant actions taken by the device. Most devices either natively allow for the device to wipe itself after a failed number of attempts, or allow the application of EMM/MDM applications to perform wiping actions after a predetermined number of failed login attempts.

Login failure actions

Mobile devices with or without MDM software can typically be configured to perform actions based on serial unsuccessful login attempts. Appropriate actions to configure may be dependent on the data resident on the device and the connectivity method employed by the device. Most devices can be configured to delete all data on the device and/or issue an alert to the network if a number of incorrect passwords are entered. This is a very advantageous feature, however specific configuration of the number of attempts and resultant action must be considered against the state of the device after an unsuccessful attempt action is triggered. A full device wipe will typically leave the device in a fully or partially non-functional state which could introduce risk if part of the intended use is time critical phone calls. Where possible, full device wipe associated with unsuccessful attempts at the device level password should be configured but the number of invalid attempts may exceed the CJIS Security Policy at the device level if all CJI on the device is protected by an additional layer of encryption protected by a subsequent secure application authentication method that is technically prevented (via complexity rules or entry rules) from being the same as the device level authentication and the secure application is configured in accordance with the policy and also contains a secure data wipe capability after a specified number of incorrect authentication attempts.

System use Notification (CJIS Policy reference 5.5.4)

Agency policy should include specific mandatory language consistent with the CJIS Security Policy to identify the device restrictions and consent. However, due to screen size limits, some mobile devices may not be technically capable of displaying the full text used with traditional operating systems. To achieve compliance agencies should contact their legal department for appropriate wording of a short version of the system use notification that can be set to display within the constraints of the device lock screen. This may be accomplished through embedding the text into an image displayed on the lock screen or some other external device labeling method if the device does not permit sufficient text to be displayed.

In a BYOD environment or mixed (agency owned and BYOD), it may be necessary to develop or deploy custom applications that can achieve compliance with the system use notification upon access and prior to any CJI access being allowed.

Session Lock (CJIS Policy reference 5.5.5)

Due to the portable nature of mobile devices the session lock limit in the general CJIS Security Policy may be excessive in the mobile environment for certain device functions and insufficient for other functions based on intended device usage. Agencies should examine the minimum lock time practical for all mobile devices based on their employment scenario and ease for which a user can manually lock the device. The actual session lock times should be adjusted as appropriate to the device type, device operational location, and the data accessible on the device when unlocked. Pocket size devices are at greatest risk if screen lock times are insufficient, however, for devices used in emergency response or communication, extended lock times at the basic device level may be considered if CJI is subsequently protected by an application or web interface utilizing more stringent secure locking functions. A well designed solution may include multiple session lock settings at the device and individual application levels to ensure the CJIS Security Policy requirements are met for CJI access, while other device functions are accessible under different session lock configurations.

Device WiFi Policy

Specific WiFi configuration policy should be developed based on the intended use environment and data access requirements for the device. The policy should explicitly cover configuration of device connections. Technical methods specific to the mobile technologies may need to be implemented to ensure all mobile devices are compliant with CJIS Security Policy. Current CJIS Security Policy provides detailed configuration requirements for WiFi connections, however it was originally intended for defining requirements for fixed infrastructure WiFi (802.11) supporting wireless within a facility. The security requirements identified for fixed infrastructure installations are applicable to mobile usage, however there are several mobile specific scenarios where the requirements may not be clear. The following sections identify areas not specifically covered in the existing policy that will require special handling to ensure wireless connections are compliant.

Hotspot capability

Many mobile devices now include the capability to activate an internal WiFi hotspot that allows other devices to connect through the hosting device to the internet over the devices cellular radio. While this is a potentially valuable capability when multiple law enforcement devices may need localized internet or network access, mobile hotspots should be configured as consistent with the CJIS Security Policy on wireless access points. Connections must only be accepted from known and approved devices in order to protect the integrity of the hosting device as well as the communications security of other connected devices. Since most mobile hotspots are not technically capable of providing the device authentication required for infrastructure wireless, use of mobile hotspot capability should assume the overall portable WiFi network itself is not secure and CJI should not be transmitted or exposed on the network without appropriate encryption.

Connection to public hotspots

There are significant risks to connecting to public wireless access points. Rogue access points masquerading as legitimate public access points may allow for man-in-the-middle, eavesdropping, and session hijacking attacks. While not specifically prohibited in the current CJIS Security Policy, it is recommended that connection to public internet access points be technically restricted by device configuration or MDM systems if possible. CJI access mechanisms from mobile devices should include robust authentication methods specifically designed to prevent interception or hijacking of CJI or user information through the use of a rogue access point masquerading as a legitimate public wireless access point. Transmission encryption alone may not provide sufficient protections when device connections originate at public hotspots. Since the public hotspot controls access to all network services at the connection point (e.g. Domain Name System) attacks against the transmission path are possible that would not normally be feasible in a fixed environment where communications exist between two secured network enclaves.

Cellular Service abroad

If mobile devices are used outside of the United States, especially if connected to foreign cellular networks, specific handling procedures may need to be developed for the use of the device while abroad and the assessment or configuration check of the device state once the devices are returned to the United States. Certain device internal functions on cellular devices may be

modified or compromised by the cellular carrier as the devices are intended to have certain parameters configured by the cellular service provider which is considered a ‘trusted’ entity by the device. Cellular carriers within the United States are constrained by United States laws regarding acceptable modifications to devices. Similar legal constraints cannot be assumed to exist in some areas of the world where laws and regulations for data and personal privacy may allow cellular carriers significantly more leeway in changes made to devices on their networks.

Security plans involving cellular connected devices that will be connected to foreign cellular networks should include technical and policy controls to ensure device use while abroad, data resident on the device while abroad, and the software integrity of the device once returned to the United States are all appropriate to the specific device and threat levels associated with the expected foreign travel. This should explicitly include considerations for devices in which an internal subscriber identity module (SIM) card is inserted into the device to obtain Global System for Mobile (GSM) cellular connections abroad to ensure any residual data on the SIM card is properly purged. Additionally, incident handling procedures may need to specify more stringent responses to even momentary loss of device control, and it may not be possible to assume tracking, anti-theft, and remote data wipe functions that work in the United States would be functional in all potentially visited geographic and political regions.

Bluetooth

Mobile devices utilizing Bluetooth should be evaluated for their ability to comply with the CJIS Security Policy Bluetooth requirements prior to acquisition. This includes the data device itself and any authorized Bluetooth accessories which will be associated to the device. While the technical security in current versions of Bluetooth is significantly stronger than legacy versions, mis-configuration of devices can still pose a significant threat in the mobile environment. If not specifically utilized for a required purpose, it would likely be most cost effective to disable or restrict the device Bluetooth radio utilizing device configurations or an MDM product. Additionally, the using agency may need to develop technically extensive training or user awareness programs to ensure use of Bluetooth capability does not render the device out of compliance if device users have the ability to make Bluetooth associations to the device. Specific instructions or guidance for specific devices could be developed to ensure all implementations are compliant.

Voice/Voice over IP (VoIP)

Cellular voice transmissions are distinctly different at the technical level than Voice over IP (VoIP) transmissions using voice/video applications (e.g. Facetime, Skype). The use of VoIP is not specifically granted the exemption identified in CJIS Security Policy Section 5.5.7.3.2. Agencies wishing to use capability of this type should ensure the specific technical implementation complies with the Policy on authentication and data encryption.

Chat/Text

Device integrated chat/texting applications and many common third party chat applications authenticate and are identified using embedded passwords or the device identifier only. These functions should not be considered secure or appropriate for transmission of CJI data. Texting functions that utilize a cellular service providers Short Message Service (SMS) or Multimedia Messaging Services (MMS) functions do not constitute a secure transmission medium. Third party applications utilizing appropriate encryption and authentication methods independent of the

device password/PIN may provide a compliant solution where the device integrated utilities are will not provide a compliant solution.

Administrative Access

Local administrative access to the mobile device, regardless of device category should be restricted by some mechanism. For traditional operating systems, configuration of a separate administrative account other than that used for normal logins to the device is an acceptable method to ensure appropriate access permissions to the mobile user for which they are authorized. However for limited functionality mobile operating systems (e.g. Android, Apple iOS) internal permissions and accounts assume a single authorized device user with explicitly defined permissions. Those permissions may be modified through policy applied to the device, but are typically global to the device itself. As a result, to ensure appropriate separation of access permissions, it may be required to ensure specific applications or software on the device are configured with individual authentication methods to separate application data from ‘general user’ access. Without additional authentication at the application level, access to specific application data would be available to any user with the ability to unlock the device. This may be appropriate in some scenarios with a high degree of assurance that the device can only be accessed by a single user, but sufficiently stringent device passwords and short screen lock times may prove problematic for practical use of some device functions. An alternate method to ensure strict separation of ‘routine’ device functions which may be accessed by multiple individuals (e.g. phone function if loaned to someone for a critical call) is to ensure any method used to access or store CJI has a separate and more stringent authentication method configured with rules that make it impossible to use the same authentication credential (e.g. PIN/Password) on both the device authentication and the application or function with access to CJI.

Rooting/Jailbreaking

‘Rooting’ (Android OS) or ‘Jailbreaking’ (Apple iOS) refer to intentional modifications to the mobile device operating system in order to grant the device user or an installed application elevated control that would not normally exist on the device. The security model internal to the various mobile device architectures vary significantly, however the common effect of rooting or jailbreaking the devices is to bypass many or all of the built in security features. The security feature bypass may be universal to all device features and installed applications once completed. Intentionally rooting or jailbreaking mobile devices should be avoided in any scenario as it potentially defeats all built-in data access and segregation controls on the device. Additionally the rooting or jailbreaking process itself has a heightened risk of introducing malicious code as part of the process, and also substantially increases the risk for malware to infect the device through user action. Extreme caution should be used if software is being installed that requires the devices to be rooted or jailbroken for the software or application to function. This is inclusive of purported security software that requires a rooted or jailbroken device to function. For example, on both the Android and Apple iOS platforms, the built-in security features for data access and memory segmentation prevent the effective operation of ‘traditional’ anti-virus and intrusion detection/prevention software. Software or applications purporting to perform these functions but requiring rooting or jailbreaking of the device and may actually accomplish the anti-virus or IDS/IPS function but are also likely to significantly increase the overall risk associated to the device by effectively disabling most or all of the integrated security features. A careful risk-based assessment should be conducted by a trained security professional prior to allowing the operation of any rooted or jailbroken mobile devices regardless of intended use.

Significant compensating controls would be required to return a rooted or jailbroken device to minimal compliance with most of the CJIS Security Policy and would likely not be a cost effective approach.

NOTE: There is a distinction between rooting a 'stock' Android installation vice the installation of a separately supported secure operating system. There are secure versions of Android available or that can be developed based on the open source Android source code and compiled for installation on a particular hardware device. Installation of a secure, supported mobile operating system that replaces the device original operating system may significantly enhance the security of the device and should not be confused with 'rooting' and Android installation. Due to the close integration of operating system security with hardware elements, and the proprietary nature of Apple source code, there are not currently separate 'secure' versions of the Apple iOS and it is unlikely they will be developed.

Identity and Authentication

Due to the technical methods used for identity and authentication on many limited functionality mobile operating systems, achieving compliance to CJIS Security Policy may require layering of identification and authentication mechanisms. With the complexity and large number of potential identity and authentication solutions in the mobile environment emphasis must be placed on designing secure identity management and authentication architecture prior to the selection of individual devices or applications. Failure to consider a robust identity and authentication scheme as part of system design or acquisition will significantly increase the risk of subsequent noncompliance with CJIS Security Policy and potential added costs for a remedial solution. Many identity and authentication schemes used by existing commercial applications may make claims that appear to be consistent with CJIS Security Policy Advanced Authentication requirements, however, extreme care must taken to ensure the actual technical implementation is compliant with policy.

Utilizing Unique device Identification

Some commercial applications and features integrated with some mobile operating systems permit the mobile device to be uniquely identified in a cryptographically robust manner. Any authentication schema that considers the possession of the mobile device as a factor in uniquely identifying and authenticating a CJIS authorized user must also include factors beyond than mere possession of the device. Larger form factor devices that cannot be carried on the person of the authorized user should not rely on possession of the device as an identifying factor, but may still include identifying capability within the device to provide assurance that the device itself is an authorized device. This should still be coupled with multi-factor advanced authentication to the device itself or the application hosting CJI. Coupling unique device authentication with robust advanced authentication of the user provides a high degree of confidence that both the specific device and the operator of the device are correctly identified. Utilizing device unique identification in order to authorize initial connections from the remote device back to the CJI hosting system or enclave provides additional protection to the CJI hosting system to reduce the attack surface of the hosting system and should be considered a good practice, but not in itself an authentication mechanism for the device user.

Certificate Use

One method for uniquely identifying mobile devices is to place part of a public key pair on the device in the form of a public key certificate. While there is value to ensuring the device itself can authenticate to a system supplying CJI, and may provide a critical layer of identification or authentication in a larger scheme, a certificate alone placed on the device should not be considered valid proof that the device is being operated by an authorized CJIS user, only that the device itself is authorized to host CJIS users. Additional user identification and authentication should be used to supplement any device certificate installed. Using a PIN or password separate from the device login to ‘unlock’ the certificate from cryptographic storage within a secure application will provide an additional layer of security and may increase the confidence level the device is being used by the intended user. However, use of public/private key pairs or pre-shared encryption keys can be utilized as part of an architecture to protect against certain session hijacking or man-in-the-middle attacks a mobile device may be susceptible to if connected to public internet connections.

Certificate Protections

Any certificates or cryptographic keys stored on any mobile device should include protections against the certificate or key being extracted from the device. Additionally certificates or other keys stored on mobile devices that grant the device special access or unique identification should be configured for remote wipe on demand or self deletion based on a number of unsuccessful login or access attempts. Alternatively, methods may be used to revoke or invalidate the unique certificate or keys associated with a device.

Minimum Password/Pin (Reference CJIS Security Policy Section 5.6.2.1)

The minimum password protections identified in the CJIS Security Policy may not be appropriate for the device PIN/password due to immediate access requirement for some device functions (e.g. phone function) secured by the device PIN/password and the difficulty to enter a complex password under emergency conditions on a small screen. In cases where the risk of a complex password on the device itself is deemed significant, a layered authentication approach may be necessary where CJI or access to CJI is protected via one or more additional layers of access control beyond the device PIN/password. In cases where the CJI or access to the CJI is cryptographically segregated from applications accessible using the device level PIN/Password (e.g. secure application or secure browser vice the built-in browser) the authentication mechanism for the secure application or browser may satisfy the CJIS Security Policy requirements if fully compliant as a stand-alone application.

Configuration Management

Due to the potential for inconsistent network access or monitoring capability on mobile devices, methods used to monitor and manage the configuration of traditional full featured operating systems may not function properly on limited function mobile operating systems. Configuration Management systems in the mobile environment may be designed in order to duplicate some of the functions typically performed by traditional anti-malware systems that will not function properly on some mobile operating systems.

Mobile Device Management (MDM)/Enterprise Mobility Management (EMM)

MDM and EMM systems and applications coupled with device specific technical policy can provide a robust method for device configuration management if properly implemented. MDM capabilities include the application of mandatory policy settings on the device, detection of

unauthorized configurations or software/applications, detection of rooting/jailbreaking of the device, and many other security policy related functions. In many cases, the most cost effective way to achieve CJIS Security Policy compliance on mobile devices is the selection of MDM or EMM applications and infrastructure appropriate to the mobile operating systems and intended access to CJI on the mobile devices. MDM/EMM functions may be applicable to most of the CJIS Security Policy requirements and allow for significant compensating controls in areas where traditional methods of CJIS Security Policy compliance are not technically feasible. Section 5.5.7.3.3 of the CJIS Security Policy specifies the minimum functions required for MDM. However, careful selection of the MDM product will potentially provide a cost effective method for additional areas of compliance in the access, auditing, incident response, authentication, media protection and system integrity sections of the CJIS Security Policy.

Device Backups/Images

Device images and backups provide protection against data loss, but also provide a method to quickly recover a device after damage or potential compromise. Due to an inherently limited ability to access the internal file structure of mobile devices, it can be difficult to easily identify a device compromise or illicit modification of the device. Some device imaging and assessment software may provide a secondary forensic capability, especially if there is intent for the device to be used outside the United States.

Bring Your Own device (BYOD) employment

BYOD environments pose significant challenges to the management of secure device configurations. In many cases it may be impossible to apply effective security that is acceptable to the device owner or it may require extremely costly compensating controls to allow access to CJI on personally owned devices. While allowed by the CJIS Security Policy, agencies are advised to conduct a detailed cost analysis of the ancillary costs of compliance with CJIS Security Policy on personally owned devices when they are approved for use. In some cases, a BYOD user may agree to abide by the same device configurations and limitations as imposed on an agency owned device, but signed user agreements should still be in place to ensure the agency has a legal right to recover or clear the device of all data prior to device disposal or employee termination. In other cases, robust secure applications may provide acceptable levels of compliance in a BYOD environment for limited CJI access but application design and architecture should assume the device itself is un-trusted. If MDM/EMM software capable of detecting rooting or jailbreaking of the device is not installed, any CJIS or data access occurring from the device is at a substantially higher risk of compromise.

Configurations and tests

Common configurations specific to all employed mobile devices should be developed to ensure compliance. Configuration tests should be developed and executed on all versions of mobile devices under all possible connectivity scenarios to ensure CJIS Security Policy compliance under all expected operating conditions. Since mobile devices can expect to operate in different physical and network environments, testing and validating correct security functions is more critical than on fixed computing platforms. Additionally, security functions that function properly on one version of a mobile operating system on a particular device may not function in the same manner even on the same version on a different device or a different version on the same device.

Media Protection

Some mobile device hardware platforms include the ability to add removable storage in the form of memory cards. This function is primarily related to Android and Windows mobile platforms and is intentionally limited on Apple devices, but may be possible through certain application functions. While the Android platform performs robust cryptographic separation of data stores between applications within the 'internal' storage of the device, the Android OS does not provide secure separation of data stores on 'external' storage. Some Android hardware devices include additional storage hardwired inside the device that is classified by the operating system as external storage and the normal separation between applications accessing that storage is not applied. Each potential device considered for acquisition must be assessed regarding specific 'external' media protection requirements which may actually include built-in media or storage.

Protection of device connected media

As a result of the limited protection and encryption capabilities applied to device removable media and SIM cards for cellular provisioning that include onboard data storage, all externally removable media or memory should be handled consistently with the CJIS Security Policy on media protection.

Encryption for device media

While most mobile operating systems have the capability to encrypt internal storage, it may require specific device settings to be enabled. All mobile device storage should meet the encryption requirements identified for media in the CJIS Security Policy. Specific settings may need to be applied to ensure proper encryption is actually employed. Additionally, the device built-in encryption capability is typically tied to the device PIN or password. Depending on the device PIN or password requirements the integrated encryption may be easily bypassed by password guessing and appropriate consideration should be made to ensure additional encryption protected by advanced authentication methods be applied to all CJI.

Physical Protection

Due to small form factors and the fact that mobile devices are often stored in lower security areas and vehicles, physical protection of the devices must be considered in both policy and training. Physical protections will often be the responsibility of the assigned device user and physical protections typically inherited by individual information systems from a secure facility will not be available to mobile devices which will require compensating controls to achieve compliance.

Device Tracking/Recovery

MDM software as well as some integrated mobile operating system functions may allow tracking of stolen or lost devices via 'always-on' cellular data connections and the devices built-in GPS. Device tracking with WiFi only or 'on-demand' cellular access may not be reliable. Enabling device tracking capabilities, while not a replacement for secure storage, could be a compensating control used to substantially reduce overall device risk in some scenarios. Device tracking is not currently required in the CJIS Security Policy but should be applied to agency owned devices where possible as a risk mitigation factor. Enabling of device tracking on personally owned devices in a BYOD environment may raise employee privacy concerns and should be considered only for critical systems with the full knowledge of the employee and concurrence of the legal department. This is an enhanced risk that must be accepted for BYOD employments and should be considered when allowing BYOD employment. Device tracking is available for both limited

function mobile operating systems as well as traditional operating systems installed on laptop devices.

Access to device tracking software or applications within the organization should be controlled with limits and formal processes required to initiate a tracking action. It is advisable to include appropriate clauses in user agreements under what conditions and controls the organization applies to device tracking.

Devices utilizing unique device identification/certificates

Devices utilizing unique device identification or have installed certificates may require additional physical protection and/or additional incident handling steps in case of device loss in order to ensure the device unique identifier or certificate is immediately revoked or disabled. Additional physical protection rules or policy would be appropriate for any device which contains access mechanisms tied to the device.

System Integrity (CJIS Policy Section 5.10)

Managing system integrity on limited function mobile operating systems may require methods and technologies significantly different from traditional full feature operating systems. In many cases the requirements of Section 5.10 of the CJIS Security Policy cannot be met with a mobile device without the installation of a third party MDM or EMM application and supporting server infrastructure.

Patching/Updates

MDM software may provide compliance to the Section 5.10.4.1 patch management requirements for particular platforms and software versions. However, devices without ‘always-on’ cellular connections may not be reachable for extended periods of time by the MDM or EMM solution either to report status or initiate patching. Supplementary or manual device accountability methods may need to be implemented to account for devices without persistent connections to ensure their patch and update state is current. Alternatively, some patches or system updates may not be practical over cellular connections and will require connection of devices to a WiFi network. Compliance with CJIS Security Policy requirements through purely technical means may not be practical and considerations should be made for aggressive management of devices through training and mandatory periodic connection of devices to organizationally managed WiFi networks.

TECHNOLOGY NOTE: Apple and Android based devices have different potential issues regarding device operating system updates. Apple maintains support for updating the operating system on Apple hardware for several device generations (typically 3-5 years) and provides a robust mechanism for system updates. However, updates to Android based systems are driven by the individual device manufacturer which may or may not support regular updates to current Android operating system versions. Additionally, different Android device vendors may offer updates/upgrades to the Android operating system on different schedules, which can complicate environments utilizing Android devices from multiple manufacturers.

Malicious code protection/Restriction of installed applications and application permissions

MDM or EMM software will typically allow restrictions on installed applications. One of the few effective attack vectors to compromise mobile operating systems is to manipulate the device user to install a malicious application. Even though the application may be restricted from

accessing other application data, it may have some access to common data stores on the device and access to device functions (e.g. GPS, microphone, and camera) that are undesirable. Unrestricted installation of applications by the device user could pose a significant risk to the device.

Malicious code protection using traditional virus scanning software is technically infeasible on most limited function mobile operating systems that are not rooted or jailbroken. The integrated data and program separations prevent any third party installed program from accessing or 'scanning' within another application data container. Even if feasible, power and storage limitations would be prohibitive in the effect on device battery life and storage capacity on most mobile devices. However, the cryptographic separation between applications and effective application virtualization technologies built into common mobile operating systems partially compensate for the lack of traditional virus scanning technologies. Appropriately configured MDM software is capable of checking the installed applications on the device and reporting the software inventory to a central management console in a manner analogous to traditional virus scan detection of unauthorized software. This behavior is analogous to the software inventory performed by anti-virus products and can provide a high degree of confidence that only known software or applications are installed on the device. While it is theoretically possible to bypass the application sandboxing and data segregation protections to compromise a mobile device through the web browser, the attack methods required are significantly more advanced than those required for a traditional full featured operating system. Malicious code protections on the device web browser can be enforced through the use of a properly protected web proxy which the device is configured to use as a mandatory device policy. The most common method of malicious code installation is enticing the user to manually install the malicious app which can be mitigated on organizational devices using an MDM or other application installation restrictions which prevent the user from installing unauthorized or unknown applications. Mitigation of this issue within BYOD environments may not be possible and will present a significantly enhanced risk to the device.

TECHNOLOGY NOTE: In the particular area of application installation there is a significant difference between the behavior of Apple iOS and Android platforms. Apple cryptographically restricts the way applications will execute on the device and assigns mandatory application permissions when the application code is signed prior to release on the Apple App Store for distribution. Apps on the Apple platform must conform to Apple's policy on app behavior and cannot exceed their design permissions on access to common device functions once the app has been signed and distributed. However, the Apple method does not typically advertise the precise internal permissions granted to the app to the user prior to installation. At runtime, the app is required to request user permission to access certain device functions, and the user may agree or not agree, which may introduce risk if they are unaware of what they are agreeing to allow. Unsigned or un-trusted apps are cryptographically prevented from executing on non-jailbroken iOS devices. Apple provides a mechanism for organizations to distribute custom apps within an organization with equivalent protections but all receiving devices must have a special certificate installed that will only allow official App Store and the organization custom apps to execute.

Conversely, the Android platform, while also requiring app code signing, allows for self-signed code which can be distributed by means other than an official app store and execute on any Android device. Application permissions are presented to the user once at app installation but ramifications of agreement to certain app permissions may not be obvious to a non-technical

user. Permissions in the Android model require user acceptance of all app requested permissions or the app is denied installation, which can result in unwise user acceptance of excessive permissions in order to gain functionality provided by the app.

On either platform user installation of applications can significantly change the security state of the device. Applications may be able to transmit and receive data or share device common data with other devices over the network or local WiFi or Bluetooth connection. On either platform it is highly desirable to limit allowable applications to a pre-approved pool of apps via MDM or organizational App store structures and device policy. However, the risks associated with uncontrolled app installation is several orders of magnitude greater on Android based devices.

WARNING: Rooted or jailbroken devices are modified in such a manner that the built in protections against malicious code are effectively disabled. A rooted or jailbroken device would require significant and costly compensating controls to achieve compliance.

Firewall/IDS capability

Traditional device or “personal” firewalls as identified in CJIS Security Policy Section 5.10.4.4 may not be practical on limited function mobile device operating systems but significant compensating controls are available. By default, mobile device operating systems have a limited number of system services installed and carefully controlled network access. To a certain extent the mobile operating system performs similar effective functions as a personal firewall would perform on a general purpose operating system. Potential compensating controls for the five (5) personal firewall requirements specified in Section 5.10.4.4 are listed below:

1. Manage Program Access to the Internet: On agency controlled devices with an MDM, limiting the apps installed on the device will effectively perform the same function. Since no software or apps can be installed without MDM approval a robust approval process can effectively ensure internet access is only granted to approved apps. Built-in apps and functions can also be limited on network access by the MDM.
2. Block unsolicited requests to connect to the user device: Default configurations for mobile operating system platforms typically block incoming requests. It is possible to install an app that may ‘listen’ on the network and accept connections, but the same compensating control identified in item 1 will mitigate the likelihood of that occurring.
3. Filter incoming traffic by IP address or protocol: Protocol filtering effectively occurs due to the limited function of the operating system as long as no installed application opens network access ports. The mitigations in 1 effectively compensate for this control as well.
4. Filter incoming traffic by destination ports: Same as 3.
5. Maintain an IP traffic log: This may not be technically feasible on most mobile operating system platforms as maintaining this log would require access to lower level operating system functions that are not accessible unless the device is rooted or jailbroken. However, individual Apps that communicate over the network or accept connections from the network may permit logs of IP traffic associated to that application to be stored.

Spam Protection

Spam guards installed on corporate or organizational email systems may effectively accomplish the spam protection requirements for the CJIS Security Policy on mobile devices if properly configured to block spam before delivery to the device. If no upstream spam guard is installed on the mail server the mobile devices accesses, the device may not have adequate spam protection. Additionally access to internet based email (web mail) would need to be restricted to web mail with appropriate spam and/or antivirus protections to ensure compliance.

Periodic system integrity checks

One method to compensate for the technical infeasibility of traditional anti-virus and malicious code protection is to install an MDM that performs periodic system integrity checks that validate device configuration and status against an approved baseline. Deviations may provide indicators of potential device compromise or mis-configuration.

APPENDIX H SECURITY ADDENDUM

The following pages contain the legal authority, purpose, and genesis of the Criminal Justice Information Services Security Addendum (H2-H4); the Security Addendum itself (H5-H6); and the Security Addendum Certification page (H7).

**FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM**

**Legal Authority for and Purpose and Genesis of the
Security Addendum**

Traditionally, law enforcement and other criminal justice agencies have been responsible for the confidentiality of their information. Accordingly, until mid-1999, the Code of Federal Regulations Title 28, Part 20, subpart C, and the National Crime Information Center (NCIC) policy paper approved December 6, 1982, required that the management and exchange of criminal justice information be performed by a criminal justice agency or, in certain circumstances, by a noncriminal justice agency under the management control of a criminal justice agency.

In light of the increasing desire of governmental agencies to contract with private entities to perform administration of criminal justice functions, the FBI sought and obtained approval from the United States Department of Justice (DOJ) to permit such privatization of traditional law enforcement functions under certain controlled circumstances. In the Federal Register of May 10, 1999, the FBI published a Notice of Proposed Rulemaking, announcing as follows:

1. Access to CHRI [Criminal History Record Information] and Related Information, Subject to Appropriate Controls, by a Private Contractor Pursuant to a Specific Agreement with an Authorized Governmental Agency To Perform an Administration of Criminal Justice Function (Privatization). Section 534 of title 28 of the United States Code authorizes the Attorney General to exchange identification, criminal identification, crime, and other records for the official use of authorized officials of the federal government, the states, cities, and penal and other institutions. This statute also provides, however, that such exchanges are subject to cancellation if dissemination is made outside the receiving departments or related agencies. Agencies authorized access to CHRI traditionally have been hesitant to disclose that information, even in furtherance of authorized criminal justice functions, to anyone other than actual agency employees lest such disclosure be viewed as unauthorized. In recent years, however, governmental agencies seeking greater efficiency and economy have become increasingly interested in obtaining support services for the administration of criminal justice from the private sector. With the concurrence of the FBI's Criminal Justice Information Services (CJIS) Advisory Policy Board, the DOJ has concluded that disclosures to private persons and entities providing support services for criminal justice agencies may, when subject to appropriate controls, properly be viewed as permissible disclosures for purposes of compliance with 28 U.S.C. 534.

We are therefore proposing to revise 28 CFR 20.33(a)(7) to provide express authority for such arrangements. The proposed authority is similar to the authority that already exists in 28 CFR 20.21(b)(3) for state and local CHRI systems. Provision of CHRI under this authority would only be permitted pursuant to a specific agreement with an authorized governmental

agency for the purpose of providing services for the administration of criminal justice. The agreement would be required to incorporate a security addendum approved by the Director of the FBI (acting for the Attorney General). The security addendum would specifically authorize access to CHRI, limit the use of the information to the specific purposes for which it is being provided, ensure the security and confidentiality of the information consistent with applicable laws and regulations, provide for sanctions, and contain such other provisions as the Director of the FBI (acting for the Attorney General) may require. The security addendum, buttressed by ongoing audit programs of both the FBI and the sponsoring governmental agency, will provide an appropriate balance between the benefits of privatization, protection of individual privacy interests, and preservation of the security of the FBI's CHRI systems.

The FBI will develop a security addendum to be made available to interested governmental agencies. We anticipate that the security addendum will include physical and personnel security constraints historically required by NCIC security practices and other programmatic requirements, together with personal integrity and electronic security provisions comparable to those in NCIC User Agreements between the FBI and criminal justice agencies, and in existing Management Control Agreements between criminal justice agencies and noncriminal justice governmental entities. The security addendum will make clear that access to CHRI will be limited to those officers and employees of the private contractor or its subcontractor who require the information to properly perform services for the sponsoring governmental agency, and that the service provider may not access, modify, use, or disseminate such information for inconsistent or unauthorized purposes.

Consistent with such intent, Title 28 of the Code of Federal Regulations (C.F.R.) was amended to read:

§ 20.33 Dissemination of criminal history record information.

- a) Criminal history record information contained in the Interstate Identification Index (III) System and the Fingerprint Identification Records System (FIRS) may be made available:
 - 1) To criminal justice agencies for criminal justice purposes, which purposes include the screening of employees or applicants for employment hired by criminal justice agencies.
 - 2) To noncriminal justice governmental agencies performing criminal justice dispatching functions or data processing/information services for criminal justice agencies; and
 - 3) To private contractors pursuant to a specific agreement with an agency identified in paragraphs (a)(1) or (a)(6) of this section and for the purpose of providing services for the administration of criminal justice pursuant to that agreement. The agreement must incorporate a security addendum approved by the Attorney General of the United

States, which shall specifically authorize access to criminal history record information, limit the use of the information to the purposes for which it is provided, ensure the security and confidentiality of the information consistent with these regulations, provide for sanctions, and contain such other provisions as the Attorney General may require. The power and authority of the Attorney General hereunder shall be exercised by the FBI Director (or the Director's designee).

This Security Addendum, appended to and incorporated by reference in a government-private sector contract entered into for such purpose, is intended to insure that the benefits of privatization are not attained with any accompanying degradation in the security of the national system of criminal records accessed by the contracting private party. This Security Addendum addresses both concerns for personal integrity and electronic security which have been addressed in previously executed user agreements and management control agreements.

A government agency may privatize functions traditionally performed by criminal justice agencies (or noncriminal justice agencies acting under a management control agreement), subject to the terms of this Security Addendum. If privatized, access by a private contractor's personnel to NCIC data and other CJIS information is restricted to only that necessary to perform the privatized tasks consistent with the government agency's function and the focus of the contract. If privatized the contractor may not access, modify, use or disseminate such data in any manner not expressly authorized by the government agency in consultation with the FBI.

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A-130 as “security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.”

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.

1.00 Definitions

1.01 Contracting Government Agency (CGA) - the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.

1.02 Contractor - a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

2.00 Responsibilities of the Contracting Government Agency.

2.01 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. The acknowledgement may be signed by hand or via digital signature (see glossary for definition of digital signature).

3.00 Responsibilities of the Contractor.

3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed and all subsequent versions), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

4.00 Security Violations.

4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

4.02 Security violations can justify termination of the appended agreement.

4.03 Upon notification, the FBI reserves the right to:

- a. Investigate or decline to investigate any report of unauthorized use;
- b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CGA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

5.00 Audit

5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

6.00 Scope and Authority

6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.

6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

6.04 This Security Addendum may only be modified by the FBI, and may not be modified by the parties to the appended Agreement without the consent of the FBI.

6.05 All notices and correspondence shall be forwarded by First Class mail to:

Assistant Director

Criminal Justice Information Services Division, FBI

1000 Custer Hollow Road

Clarksburg, West Virginia 26306

**FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM**

CERTIFICATION

I hereby certify that I am familiar with the contents of (1) the Security Addendum, including its legal authority and purpose; (2) the NCIC Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20, and agree to be bound by their provisions.

I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which a government agency has entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

Printed Name/Signature of Contractor Employee

Date

Printed Name/Signature of Contractor Representative

Date

Organization and Title of Contractor Representative

APPENDIX I REFERENCES

White House Memo entitled “Designation and Sharing of Controlled Unclassified Information (CUI)”, May 9, 2008

[CJIS RA] *CJIS Security Policy Risk Assessment Report*; August 2008; For Official Use Only; Prepared by: Noblis; Prepared for: U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Division, 1000 Custer Hollow Road, Clarksburg, WV 26306

[FBI SA 8/2006] *Federal Bureau of Investigation, Criminal Justice Information Services, Security Addendum*; 8/2006; Assistant Director, Criminal Justice Information Services, FBI, 1000 Custer Hollow Road, Clarksburg, West Virginia 26306

[FISMA] *Federal Information Security Management Act of 2002*; House of Representatives Bill 2458, Title III–Information Security

[FIPS 199] *Standards for Security Categorization of Federal Information and Information Systems*; Federal Information Processing Standards Publication, FIPS PUB 199; February 2004

[FIPS 200] *Minimum Security Requirements for Federal Information and Information Systems*; Federal Information Processing Standards Publication, FIPS PUB 200; March 2006

[FIPS 201] *Personal Identity Verification for Federal Employees and Contractors*; Federal Information Processing Standards Publication, FIPS PUB 201-1

[NIST SP 800–14] *Generally Accepted Principles and Practices for Securing Information Technology Systems*; NIST Special Publication 800–14

[NIST SP 800–25] *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication*; NIST Special Publication 800–25

[NIST SP 800–30] *Risk Management Guide for Information Technology Systems*; NIST Special Publication 800–36

[NIST SP 800–32] *Introduction to Public Key Technology and the Federal PKI Infrastructure*; NIST Special Publication 800–32

[NIST SP 800–34] *Contingency Planning Guide for Information Technology Systems*; NIST Special Publication 800–34

[NIST SP 800–35] *Guide to Information Technology Security Services*; NIST Special Publication 800–35

[NIST SP 800–36] *Guide to Selecting Information Technology Security Products*; NIST Special Publication 800–36

[NIST SP 800–39] *Managing Risk from Information Systems, An Organizational Perspective*; NIST Special Publication 800–39

[NIST SP 800–40] *Procedures for Handling Security Patches*; NIST Special Publication 800–40

[NIST SP 800–44] *Guidelines on Securing Public Web Servers*; NIST Special Publication 800–44

- [NIST SP 800–45] *Guidelines on Electronic Mail Security*; NIST Special Publication 800–45, Version 2
- [NIST SP 800–46] *Security for Telecommuting and Broadband Communications*; NIST Special Publication 800–46
- [NIST SP 800–48] *Wireless Network Security: 802.11, Bluetooth, and Handheld Devices*; NIST Special Publication 800–48
- [NIST SP 800–52] *Guidelines on the Selection and Use of Transport Layer Security*; NIST Special Publication 800–52
- [NIST SP 800–53] *Recommended Security Controls for Federal Information Systems*; NIST Special Publication 800–53, Revision 2
- [NIST SP 800–53A] *Guide for Assessing the Security Controls in Federal Information Systems, Building Effective Security Assessment Plans*; NIST Special Publication 800–53A
- [NIST SP 800–58] *Security Considerations for Voice over IP Systems*; NIST Special Publication 800–58
- [NIST SP 800–60] *Guide for Mapping Types of Information and Information Systems to Security Categories*; NIST Special Publication 800–60, Revision 1, DRAFT
- [NIST SP 800–63–1] *Electronic Authentication Guideline*; NIST Special Publication 800–63–1; DRAFT
- [NIST SP 800–64] NIST Special Publication 800–64
- [NIST SP 800–66] *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA)*; NIST Special Publication 800–66
- [NIST SP 800–68] *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist*; NIST Special Publication 800–68
- [NIST SP 800–70] *Security Configuration Checklists Program for IT Products*; NIST Special Publication 800–70
- [NIST SP 800–72] *Guidelines on PDA Forensics*; NIST Special Publication 800–72
- [NIST SP 800–73] *Integrated Circuit Card for Personal Identification Verification*; NIST Special Publication 800–73; Revision 1
- [NIST SP 800–76] *Biometric Data Specification for Personal Identity Verification*; NIST Special Publication 800–76
- [NIST SP 800–77] *Guide to IPSec VPNs*; NIST Special Publication 800–77
- [NIST SP 800–78] *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*; NIST Special Publication 800–78
- [NIST SP 800–81] *Secure Domain Name System (DNS) Deployment Guide*; NIST Special Publication 800–81
- [NIST SP 800–84] *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*; NIST Special Publication 800–84

- [NIST SP 800–86] *Guide to Integrating Forensic Techniques into Incident Response*; NIST Special Publication 800–86
- [NIST SP 800–87] *Codes for the Identification of Federal and Federally Assisted Agencies*; NIST Special Publication 800–87
- [NIST SP 800–96] *PIV Card / Reader Interoperability Guidelines*; NIST Special Publication 800–96
- [NIST SP 800–97] *Guide to IEEE 802.11i: Robust Security Networks*; NIST Special Publication 800–97
- [NIST SP 800–121] *Guide to Bluetooth Security*, NIST Special Publication 800-121
- [NIST SP 800–124] *Guidelines on Cell Phone and PDA Security*, NIST Special Publication 800-124
- [NIST SP 800–144] *Guidelines on Security and Privacy in Public Cloud Computing*; NIST Special Publication 800-144
- [NIST SP 800–145] *The NIST Definition of Cloud Computing*; NIST Special Publication 800-145
- [NIST SP 800–146] *Cloud Computing Synopsis and Recommendations*; NIST Special Publication 800-146
- [OMB A–130] *Management of Federal Information Resources*; Circular No. A–130; Revised; February 8, 1996
- [OMB M–04–04] *E-Authentication Guidance for Federal Agencies*; OMB Memo 04–04; December 16, 2003
- [OMB M–06–15] *Safeguarding Personally Identifiable Information*; OMB Memo 06–15; May 22, 2006
- [OMB M–06–16] *Protection of Sensitive Agency Information*; OMB Memo 06–16; June 23, 2006
- [OMB M–06–19] *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*; OMB Memo 06–19; July 12, 2006
- [OMB M–07–16] *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*; OMB Memo 07–16; May 22, 2007
- [Surviving Security] *Surviving Security: How to Integrate People, Process, and Technology*; Second Edition; 2004
- [USC Title 5, Section 552] *Public information; agency rules, opinions, orders, records, and proceedings*; United States Code, Title 5 - Government Agency and Employees, Part I - The Agencies Generally, Chapter 5 - Administrative Procedure, Subchapter II - Administrative Procedure, Section 552. Public information; agency rules, opinions, orders, records, and proceedings
- [USC Title 44, Section 3506] *Federal Information Policy*; 01/02/2006; United States Code, Title 44 - Public Printing and Documents; Chapter 35 - Coordination of Federal Information Policy; Subchapter I - Federal Information Policy, Section 3506

APPENDIX J NONCRIMINAL JUSTICE AGENCY SUPPLEMENTAL GUIDANCE

This supplemental guidance for noncriminal justice agencies (NCJA) is provided specifically for those whose only access to FBI CJI is authorized by legislative enactment or federal executive order to request civil fingerprint-based background checks for licensing, employment, or other noncriminal justice purposes, via their State Identification Bureau and/or Channeling agency. This guidance does not apply to criminal justice agencies covered under an active user agreement with the FBI CJIS Division for direct connectivity to the FBI CJIS Division via the FBI CJIS Wide Area Network. Examples of the target audience for this supplemental guidance include school boards, banks, medical boards, gaming commissions, alcohol and tobacco control boards, social services agencies, pharmacy boards, etc. The information below identifies the sections of the CJIS Security Policy most closely related to the NCJA's limited scope of interaction with CJI.

1. The following CJIS Security Policy sections comprise the minimum standard requirements in all situations:
 - a. 3.2.9 – Local Agency Security Officer (LASO)
 - b. 5.1.1.6 – Agency User Agreements
 - c. 5.1.1.7 – Outsourcing Standards for Channelers*
 - d. 5.1.3 – Secondary Dissemination
 - e. 5.2.1.1 – All Personnel (Security Awareness Training)
 - f. 5.3 – Incident Response
 - g. 5.4 – Auditing and Accountability
 - h. 5.8 – Media Protection
 - i. 5.9.2 – Controlled Area
 - j. 5.11 – Formal Audits **
 - k. 5.12 – Personnel Security***

* Note: Outsourcing Standard applies when contracting with channeling or outsourcing agency.

**Note: States shall periodically conduct audits of NCJAs. The FBI CJIS Division shall triennially conduct audits of a sampling of NCJAs.

*** Note: See the National Crime Prevention and Privacy Compact Council's Outsourcing Standard for Contractor background check requirements.

2. Agencies located within states having passed legislation authorizing or requiring civil fingerprint-based background checks for personnel with access to criminal history record information for the purposes of licensing or employment shall follow the guidance in Section 5.12. Agencies located within states without this authorization or

requirement are exempted from the fingerprint-based background check requirement until such time as appropriate legislation has been written into law.

3. When receiving CJI via encrypted e-mail or downloading from a web-site and subsequently storing the information as an encrypted electronic image Authorized Recipients should, in addition to all of the aforementioned sections, focus on compliance with policy sections:
 - a. 5.5.2.4 – Access Control – Encryption
 - b. 5.6 – Identification and Authentication (web-site access)
 - c. 5.10.1.2 – System and Communications Protection – Encryption
4. When receiving CJI via e-mail or retrieving CJI from a website and subsequently storing the CJI electronically, Authorized Recipients should, in addition to 1.a–1.k above, focus on compliance with policy sections:
 - a. 5.5.2.4 – Access Control – Encryption
 - b. 5.6 – Identification and Authentication
 - c. 5.7 – Configuration Management
 - d. 5.10 – System and Communications Protection and Information Integrity
5. If an NCJA further disseminates CJI via encrypted e-mail to Authorized Recipients, located outside the NCJA’s designated controlled area, the NCJA should, in addition to 1.a–3.c above, focus on compliance with policy sections:
 - a. 5.7 – Configuration Management
 - b. 5.10 – System and Communications Protection and Information Integrity
6. If an NCJA further disseminates CJI via secure website posting to Authorized Recipients, located outside the NCJA’s designated controlled area, the NCJA should focus on all sections outlined in 1.a-4.d above.

APPENDIX K CRIMINAL JUSTICE AGENCY SUPPLEMENTAL GUIDANCE

This supplemental guidance is directed toward those criminal justice agencies that have historically not been subject to audit under the CJIS Security Policy guidelines. The target audience typically gains access to CJI via fax, hardcopy distribution or voice calls; does not have the capability to query state or national databases for criminal justice information; and, may have been assigned an originating agency identifier (ORI) but is dependent on other agencies to run queries on their behalf. This guidance does not apply to criminal justice agencies covered under an active information exchange agreement with another agency for direct or indirect connectivity to the state CSA – in other words those agencies traditionally identified as “terminal agencies”. The information below identifies the sections of the CJIS Security Policy the target audience will most often encounter:

1. The following CJIS Security Policy sections comprise the minimum standard requirements in all situations:
 - a. 3.2.9 – Local Agency Security Officer (LASO)
 - b. 5.1.1.3 – Criminal Justice Agency User Agreements
 - c. 5.1.3 – Secondary Dissemination
 - d. 5.2.1.1 – Security Awareness Training
 - e. 5.3 – Incident Response
 - f. 5.4.6 – Audit Record Retention
 - g. 5.8 – Media Protection
 - h. 5.9 – Physical Security
 - i. 5.10.2 – Facsimile Transmission of CJI
 - j. 5.11 – Formal Audits*
 - k. 5.12 – Personnel Security

*Note: States shall triennially audit all CJAs

2. When receiving CJI via encrypted e-mail or downloading from a web-site and subsequently storing the information as an encrypted electronic image Authorized Recipients should, in addition to all of the aforementioned sections, focus on complying with policy sections:
 - a. 5.5.2.4 – Access Control – Encryption
 - b. 5.6 – Identification and Authentication
 - c. 5.10.1.2 – System and Communications Protection – Encryption

3. When receiving CJI via e-mail or retrieving CJI from a website and subsequently storing the CJI electronically, Authorized Recipients should, in addition to 1.a–1.k above, focus on complying with policy sections:
 - a. 5.5.2.4 – Access Control – Encryption
 - b. 5.6 – Identification and Authentication
 - c. 5.7 – Configuration Management
 - d. 5.10 – System and Communications Protection and Information Integrity

This Page Intentionally Blank

Appendix E

State Consultant Disclosure

Intentionally Blank

Instructions

State Consultant Services

Form A: Contractor's Planned Employment

And

Form B: Contractor's Annual Employment Report

Form A - Contractor's Planned Employment Form must be submitted as part of any winning Offerer's bid response before it can be submitted to the Office of the State Comptroller for approval. DCJS will coordinate with the winning Offerer(s) to complete this form.

Form B - Contractor's Annual Employment Report. Offerer/Prime Contractor agrees to annually submit Form B each year that the contract is in effect and will detail employment data for the most recent concluded State fiscal year (April 1 – March 31). Instructions for these forms follow. Form B must be submitted by May 15th of each year to the NYS Division of Criminal Justice Services, the NYS Office of the State Comptroller and the NYS Department of Civil Service. The first Form B must be submitted by May 15, 20 . The Offerer/Prime Contractor agrees to simultaneously report such information to the NYS Division of Criminal Justice Services, the NYS Office of the State Comptroller and the NYS Department of Civil Service as designated below:

NYS Division of Criminal Justice Services
Attn: Office of Financial Services, 10th Floor
Alfred E. Smith Office Building
80 South Swan Street
Albany, NY 12210-8001

NYS Office of the State Comptroller
Bureau of Contracts
Attn: Consultant Reporting
Bureau of Contracts
110 State Street, 11th Floor
Albany, NY 12236

NYS Department of Civil Service
Attn: Consultant Reporting
Empire State Plaza
Swan Street Bldg. 1
Albany, NY 12210

INSTRUCTIONS FOR COMPLETING FORM A AND B

Form A and Form B should be completed for contracts for consulting services as follows:

Form A - Contractor's Planned Employment Form (available from and submitted to the using agency, if necessary.)

Form B - Contractor's Annual Employment Report (To be completed by May 15th of each year for each consultant contract in effect at any time between the preceding April 1st through March 31st fiscal year and submitted to the Department of Civil Service, Office of the State Comptroller and procuring agency.)

- **Scope of Contract:** choose a general classification of the single category that best fits the predominate nature of the services provided under the contract.

Employment Category: enter the specific occupation(s), as listed in the O*NET occupational classification system, which best describes the employees providing services under the contract. (*Note*

*Access the O*NET database, which is available through the US Department of Labor's Employment and Training Administration, on-line at online.onetcenter.org to find a list of occupations.)*

- **Number of Employees:** enter the total number of employees in the employment category employed to provide services under the contract during the report period, including part time employees and employees of subcontractors.
- **Number of Hours:** enter the total number of hours worked during the report period by the employees in the employment category.
- **Amount Payable under the Contract:** enter the total amount paid by the State to the State contractor under the contract, for work by the employees in the employment category, for services provided during the report period.

FORM A

OSC Use Only:

Reporting Code:

Category Code:

Date Contract Approved:

State Consultant Services - Contractor's Planned Employment

From Contract Start Date Through The End Of The Contract Term

State Agency

Name: Division of Criminal Justice Services Agency Code: 01490

Contractor Name: _____ Contract Number: _____

Contract Start Date: _____ Contract End Date: _____

Employment Category	Number of Employees	Number of hours to be worked	Amount Payable Under the Contract
Total this page			
Grand Total			

Name of person who prepared this report:

Title: _____ Phone #: _____

Preparer's Signature:

Date _____

Prepared:

(Use additional pages, if necessary)

Page of

ADDENDUM ACKNOWLEDGING FORM B

Reviewed for update September 2013

Pursuant to State Finance Law §163(4)(g), Vendor agrees to annually submit Form B, State Consultant Services Contractor's Annual Employment Report to DCJS, the NYS Office of the Comptroller and NYS Department of Civil Service. A copy of Form B and instructions are attached.

The State Consultant Services Contractor's Annual Employment Report (Form B) must be submitted each year the contract is in effect and will capture actual employment data for the most recently concluded fiscal year April 1, 20__ to March 31, 20__. The first report is due May 15, 20__ and thereafter May 15th of each year.

The Vendor agrees to simultaneously report such information to the NYS Division of Criminal Justice Services, the NYS Office of the State Comptroller and the NYS Department of Civil Service as designated below:

NYS Division of Criminal Justice Services Attn: Office of Financial Services, 10 th Floor 80 South Swan Street Albany, NY 12210-8001	Office of the State Comptroller Bureau of Contracts 110 State Street, 11 th Floor Albany, NY 12236 Attn: Consultant Reporting By fax: (518) 474-8030 or (518) 473-8808	NYS Department of Civil Service Attn: Consultant Reporting Empire State Plaza Swan Street Bldg. 1 Albany, NY 12210

Authorized Signature

Date

Name (Please print)

Title (Please print)

ACKNOWLEDGEMENT CLAUSE

State of New York)
) ss.:
County of Albany)

On this ____ day of _____, 20__, before me personally came _____, to me known, who being duly sworn, deposes and says that (s)he is the _____ of the _____, the entity which executed the instrument; that (s)he was authorized by and did execute the same at the direction of said entity and that (s)he signed his/her name thereto.

Notary Public

This Page Intentionally Blank

Appendix F

Mandatory Qualifying Experience Customer Reference Questionnaire

Intentionally Blank

Appendix F

Mandatory Qualifying Experience Customer Reference Questionnaire

Introduction and Instructions - Your name has been provided by **(Enter Offerer/vendor name here)** as a reference that may be contacted about your experience with this vendor. Your input, along with other sources of information, will be used by our evaluation team to select a vendor who will implement the New York State's next generation Public Safety Credentialing and Training System "PSCTS".

This survey is comprised of two (2) parts; Part One is entitled "System Information" will be used to validate the vendors mandatory qualifying experience. Part Two is entitled "Assessment of Experience with Vendor." Please provide information regarding your system by completing both parts of the survey.

Please complete this survey in English and e-mail it back to the DCJS Procurement Office by __/__/2014 The email address is DCJSProcurement@dcjs.ny.gov

If you have questions about the survey, you may contact the NYS DCJS Procurement Office at the above mentioned e-mail address.

Part One: System Information

Customer Background Information:

Name of Company/Agency		
Company/Agency Contact		
Title		
Address		
Country		Contact Hours
Telephone # - including country code and/or area code, if applicable		Time Zone
Email:		
Installed System Name:		Software Release/Version:
Date system placed into production:		Patch Number:
Hosting of System: Customer Hosted Vendor Hosted		
Is your organization owned or controlled by (Enter Offerer/vendor name here) Yes No		
Offerer primary contractor?		

Please provide a response to each of the following questions regarding your vendor installed Public Safety Credentialing and Training System. NYS requires this information to evaluate the vendor's experience in implementing Registry Systems that are similar in size and operation to NYS's Public Safety Credentialing and Training System requirements. NYS realizes that all functions listed below may not apply to your vendor installed system.

	Question: Does your system:	Response		
1	Allows employers to perform annual validation of all employment records and report the results to records management staff; employers are able to input, update, and validate details specific to each individual employed by them currently and in the past?	Yes	No	N/A
2	Provides Gap Analysis of the validity and pending expirations of training certificates and/or qualifications; identifies gaps in employment service (including from one employer to another); and provides notification of pending expirations of certificates and/or qualifications to employers, individual record holder(s) and records management staff?	Yes	No	N/A
3	Provides self-service functionality for employees (view access for records and certificates), employers (records and data management), training instructors and academies (training record management), and administration (configuration), application is user friendly to the average non-technical individual?	Yes	No	N/A
4	System generates standard reports and statistics, including gap analysis; performs audits of training certificates and actions of system users; and the ability to define and generate ad hoc reports exists; reports can be generated in standard formats including Adobe PDF and Microsoft Excel?	Yes	No	N/A
5	Has a law enforcement database of at least 50,000 personnel records and is capable of supporting 150 concurrent users; vendor support is available at a minimum Monday to Friday 6:00 AM to 6:00 PM?	Yes	No	N/A
6	Performs a minimum of 100,000 transactions (records updates) annually and the application's user interface provides feedback in 5 seconds or less, from each key press, mouse movement or other type of input or exchange?	Yes	No	N/A
7	System has interfaces with at least one (1) exterior agency/entity e.g. FBI, State Police, Department of Health, wherein data imports and exports occur; the interface is user friendly to the average non-technical individual and capable of self service features including bulk-upload capabilities?	Yes	No	N/A
8	Contains an on-line portal or equivalent system component that automates processes for course enrollment, approval and completion, records management, certificate issuance; includes features including ability to approve and manage training academies, document retention and management, training course calendaring and self-service functionality for instructors and students. The system must allow NYS to upload training materials (records management) including but not limited to text files, audio files and/or video files with individual files upwards of 4GB in size?	Yes	No	N/A
Comments:				

Part Two Assessment of Experience with Vendor

Please use the scoring legend below to respond to each of the following questions about your experience with the vendor during your implementation and usage of the system as provided by the vendor.

When selecting a rating for each item please measure the vendor's performance against the contractual level of performance expected.

Scoring Legend:

NA = question / topic not applicable

0 = Vendor's performance in this area was completely unsatisfactory

1 = Vendor's performance in this area was minimally satisfactory.

2 = Vendor's performance in this area was average

3 = Vendor's performance in this area was better-than-average or good.

4 = Vendor's performance in this area was very good.

5 = Vendor's performance in this area was superior or excellent.

	Questions	Rating
1	Please rate your satisfaction with the vendor's performance during implementation of the system.	0 1 2 3 4 5 n/a
2	Please rate your satisfaction with the vendor's performance of any data conversion(s).	0 1 2 3 4 5 n/a
3	Please rate your satisfaction with the quality of the implementation plan that the vendor presented to your agency.	0 1 2 3 4 5 n/a
4	Please rate your satisfaction with your system availability on a daily basis.	0 1 2 3 4 5 n/a
5	How would you rate your satisfaction with the vendor's system integration with any other systems?	0 1 2 3 4 5 n/a
6	How would you rate the overall satisfaction with the flexibility to configure system features?	0 1 2 3 4 5 n/a
7	How would you rate the satisfaction with the on-line training portal or learning management system component?	0 1 2 3 4 5 n/a
8	How would you rate your overall satisfaction with vendor support responsiveness?	0 1 2 3 4 5 n/a
9	How would you rate your overall satisfaction with the support provided during upgrades and patching?	0 1 2 3 4 5 n/a

10	How would you rate your overall satisfaction with the reporting functionality provided by the System?	0 1 2 3 4 5 n/a
11	Please rate the number of system outages you have experienced?	0 1 2 3 4 5 n/a
12	Please rate the quality and completeness of vendor supplied training.	0 1 2 3 4 5 n/a
13	Please rate the length of time required to train an employee to use the system.	0 1 2 3 4 5 n/a
14	Please rate your satisfaction with the level of system security measures your vendor has provided.	0 1 2 3 4 5 n/a

Appendix G

Public Safety Credentialing and Training System Informational Tables

This Page Intentionally Blank

Table 1 - Ingenium, Current System Data Fields

The table below depicts the current system data fields. Data fields linking to a user editable field are in green font.

Item #	Table	Field	Type	Length	Comments
1	EMPCD	EMPCD_PK	Number		Job name used to designate role (police officer, peace officer, agency head)
2	EMPCD	EMPCD_NAME	String	35	Not used
3	EMPCD	EMCD_LSTUPD	Date/Time	8	Not used
4	EMPCD	EMPCD_USRNAME	String	30	System generated
5	EMPCD	EMPCD_LCK	Number		System generated
6	EMPORGHIST	EMPORGHIST_PK	Number		System generated
7	EMPORGHIST	EMPORGHIST_EMPFK	Number		Not used
8	EMPORGHIST	EMPORGHIST_ORGFK	Number		Not used
9	EMPORGHIST	EMPORGHIST_PRRY	Number		Not used
10	EMPORGHIST	EMPORGHIST_STARTDT	Date/Time		Not used
11	EMPORGHIST	EMPORGHIST_ENDDT	Date/Time		System generated
12	EMPORGHIST	EMPORGHIST_NOTE	String	255	System generated
13	EMPORGHIST	EMPORGHIST_EMPCDFK	Number		System generated
14	EMPORGHIST	EMPORGHIST_LASTUPD	Date/Time		Key field (linking)
15	EMPORGHIST	EMPORGHIST_USERNAME	String		Key field (linking)
16	EMPORGHIST	EMPORGHIST_LCK	Number		Key field (linking)
17	EVT	EVT_PK	Number		Key field (linking)
18	EVT	EVT_EVTSTATFK	Number		Key field (linking)
19	EVT	EVT_EVTLEDEFFK	Number		Employee ID (SSN)
20	EVT	EVT_VENFK	Number		Employee last name
21	EVT	EVT_PAYTERMFK	Number		Employee first name
22	EVT	EVT_DEFCLKFK	Number		Mr., Mrs.
23	EVT	EVT_NAME	String	50	Employee middle initial
24	EVT	EVT_OPENIND	Number		Employee suffix (Sr, Jr, III)
25	EVT	EVT_CNCLIND	Number		Employee title (optional)
26	EVT	EVT_CD	Number		Not used
27	EVT	EVT_MINSESREQ	Number		Not used
28	EVT	EVT_CNCLBUSDAYS	Number		Not used
29	EVT	EVT_ACTUALCOST	Number		Not used
30	EVT	EVT_MINCAP	Number		Not used
31	EVT	EVT_MAXCAP	Number		Not used
32	EVT	EVT_INSTNOTE	String	255	Not used
33	EVT	EVT_NOTE	String	255	Not used
34	EVT	EVT_STARTDT	Date/Time		Employee email
35	EVT	EVT_ENDDT	Date/Time		Not used
36	EVT	EVT_CRDTHRS	Number		Not used
37	EVT	EVT_CBTPTH	String	255	Not used
38	EVT	EVT_URL	String	255	Not used
39	EVT	EVT_LSTUPD	Date/Time		Free text notes
40	EVT	EVT_USRNAME	String	8	System generated
41	EVT	EVT_LCK	Number	30	System generated
42	GRD	GRD_PK	Number		System generated
43	GRD	GRD_NAME	String	35	Key field (linking)
44	GRD	GRD_LASTUPD	Date/Time		Key field (linking)
45	GRD	GRD_USERNAME	String	30	Primary organization designator (0/1)
46	GRD	GRD_LCK	Number		System generated

Table 1 - Ingenium, Current System Data Fields (continued)

Item #	Table	Field	Type	Length	Comments
47	GRD	GRD_MINPCTGRD	Number		System generated
48	HIERTYPE	HIERTYPE_PK	Number		System generated
49	HIERTYPE	HIERTYPE_NAME	String	35	Key field (linking)
50	HIERTYPE	HIERTYPE_LASTUPD	Date/Time		Full time or part-time status
51	HIERTYPE	HIERTYPE_USERNAME	String	30	System generated
52	HIERTYPE	HIERTYPE_LCK	Number		System generated
53	INST	INST_PK	Number		System generated
54	INST	INST_VENFK	Number		Key field (linking)
55	INST	INST_NO	String	25	Key field (linking)
56	INST	INST_TTL	String	50	Key field (linking)
57	INST	INST_LNAME	String	35	Organization (employer) name
58	INST	INST_FNAME	String	35	Free text notes
59	INST	INST_TITLE	String	5	Organization code (assigned by DCIS)
60	INST	INST_MI	String	1	Street address
61	INST	INST_SUFFIX	String	5	Address (PO Box)
62	INST	INST_STARTDT	Date/Time		City
63	INST	INST_ADD1	String	50	State
64	INST	INST_ADD2	String	50	Postal Code
65	INST	INST_INTERNALIND	Number		Literal county - agency code has county designator
66	INST	INST_CITY	String	30	Phone 1
67	INST	INST_STATE	String	2	Phone 2
68	INST	INST_COUNTRY	String	35	Facsimile
69	INST	INST_ZIP	String	10	Not used
70	INST	INST_EMAIL	String	50	Not used
71	INST	INST_PHN1	String	20	System generated
72	INST	INST_PHN2	String	20	System generated
73	INST	INST_FAX	String	20	System generated
74	INST	INST_URL	String	255	Key field (linking)
75	INST	INST_NOTE	String	255	Gender
76	INST	INST_LASTUPD	Date/Time		Not used
77	INST	INST_USERNAME	String	30	Not used
78	INST	INST_LCK	Number		Not used
79	JOB	JOB_PK	Number		Not used
80	JOB	JOB_NAME	String	50	Free text notes
81	JOB	JOB_URL	String	255	Date of birth
82	JOB	JOB_NOTE	String	255	Not used
83	JOB	JOB_LSTUPD	Date/Time	8	Weapon indicator (peace officers) (1,2,3,4)
84	JOB	JOB_USERNAME	String	30	Not used
85	JOB	JOB_LCK	Number	2	Not used
86	LEDEF	LEDEF_PK	Number		Criminal Procedure Law designation (police and peace officers)
87	LEDEF	LEDEF_LEMTDFK	Number		
88	LEDEF	LEDEF_DEFFACFK	Number		System generated
89	LEDEF	LEDEFDEFINSTFK	Number		System generated
90	LEDEF	LEDEF_DEFVENFK	Number		System generated
91	LEDEF	LEDEF_DEFPAYTERMKF	Number		Key field (linking)
92	LEDEF	LEDEF_MEDTYPEFK	Number		Key field (linking)
93	LEDEF	LEDEF_CONTYPEFK	Number		Not used
94	LEDEF	LEDEF_CD	String	30	Not used
95	LEDEF	LEDEF_NAME	String	75	Not used

Table 1 - Ingenium, Current System Data Fields (continued)

Item #	Table	Field	Type	Length	Comments
96	LEDEF	LEDEF_DESC	String	255	Not used
97	LEDEF	LEDEF_BASECOST	Number		Free text notes
98	LEDEF	LEDEF_ESTDAYS	Number		Not used
99	LEDEF	LEDEF_ESTHRS	Number		Not used
100	LEDEF	LEDEF_ESTCRDTHRS	Number		Not used
101	LEDEF	LEDEF_CNCLBUSDAYS	Number		Not used
102	LEDEF	LEDEF_INSTNOTES	String	255	Not used
103	LEDEF	LEDEF_EMPNOTES	String	255	Not used
104	LEDEF	LEDEF_CBTPATH	String	255	Not used
105	LEDEF	LEDEF_ACTIVEIND	Number		System generated
106	LEDEF	LEDEF_URL	String	255	System generated
107	LEDEF	LEDEF_LSTUPD	Date/Time		System generated
108	LEDEF	LEDEF_USRNAME	String	8	Key field (linking)
109	LEDEF	LEDEF_LCK	Number	30	Vendor (school) name
110	LEDEF	LEDEF_CBTLAUNCHMTDFK	Number	2	Contact person's title
111	OPTINST	OPTINST_FK	Number		Indicates approved status
112	OPTINST	OPTINST_TEXT1	String	255	Contact first name
113	OPTINST	OPTINST_TEXT2	String	255	Contact last name
114	OPTINST	OPTINST_TEXT3	String	255	Street address
115	OPTINST	OPTINST_TEXT4	String	255	Address (PO Box)
116	OPTINST	OPTINST_MEMO1	String	255	City
117	OPTINST	OPTINST_DT1	Date/Time		State
118	OPTINST	OPTINST_DT2	Date/Time		Postal Code
119	OPTINST	OPTINST_IND1	Number		Literal county - agency code has county designator
120	OPTINST	OPTINST_MONEY	Number		Contact email address
121	OPTINST	OPTINST_INT1	Number		Phone 1
122	OPTINST	OPTINST_FLOAT1	Number		Phone 2
123	OPTINST	OPTINST_OLE1	OLE		Facsimile
124	OPTINST	OPTINST_LASTUPD	Date/Time		Not used
125	OPTINST	OPTINST_USRNAME	String	30	Free text notes
126	OPTINST	OPTINST_LCK	Number		System generated
127	OPTVEN	OPTVEN_VENFK	Number		System generated
128	OPTVEN	OPTVEN_TXT1	String	255	System generated
129	OPTVEN	OPTVEN_TXT2	String	255	Key field (linking)
130	OPTVEN	OPTVEN_TXT3	String	255	UPS/FED EX acct #
131	OPTVEN	OPTVEN_TXT4	String	255	Not used
132	OPTVEN	OPTVEN_MEMO1	String	255	Not used
133	OPTVEN	OPTVEN_DT1	Date/Time	8	Not used
134	OPTVEN	OPTVEN_DT2	Date/Time	8	Free text notes
135	OPTVEN	OPTVEN_IND1	Number		School (initial) certification date
136	OPTVEN	OPTVEN_MONEY	Number		School renewal date
137	OPTVEN	OPTVEN_INT1	Number		School code
138	OPTVEN	OPTVEN_FLOAT1	Number		Not used
139	OPTVEN	OPTVEN_OLE1	OLE		Not used
140	OPTVEN	OPTVEN_LSTUPD	Date/Time	8	Not used
141	OPTVEN	OPTVEN_USRNAME	String	30	Not used
142	OPTVEN	OPTVEN_LCK	Number	2	System generated
143	ORG	ORG_PRNTORGFK	Number		System generated
144	ORG	ORG_HIERTYPEFK	Number		System generated

Table 1 - Ingenium, Current System Data Fields (continued)

Item #	Table	Field	Type	Length	Comments
145	ORG	ORG_CNCTEMPCK	Number		Key field (linking)
146	ORG	ORG_NAME	String	75	Key field (linking)
147	ORG	ORG_NOTE	String	255	Key field (linking)
148	ORG	ORG_CD	String	15	Key field (linking)
149	ORG	ORG_ADD1	String	50	Key field (linking)
150	ORG	ORG_ADD2	String	50	Key field (linking)
151	ORG	ORG_CITY	String	30	Key field (linking)
152	ORG	ORG_STATE	String	2	Key field (linking)
153	ORG	ORG_ZIP	String	10	Course codes
154	ORG	ORG_CNTRY	String	35	Course names (length is limiting)
155	ORG	ORG_PHN1	String	20	Not used
156	ORG	ORG_PHN2	String	20	Not used
157	ORG	ORG_FAX	String	20	Not used
158	ORG	ORG_URL	String	255	Not used
159	ORG	ORG_LEVELVAL	Number		Not used
160	ORG	ORG_LSTUPD	Date/Time	8	Not used
161	ORG	ORG_USRNAME	String	30	Free text notes
162	ORG	ORG_LCK	Number	2	Not used
163	ORGREL	ORGREL_PRNTORGFK	Number		Not used
164	ORGREL	ORGREL_ORGFK	Number		Not used
165	ORGREL	ORGREL_LASTUPD	Date/Time		Not used
166	ORGREL	ORGREL_USERNAME	String	30	System generated
167	ORGREL	ORGREL_LCK	Number		System generated
168	SKL	SKL_PK	Number		System generated
169	SKL	SKL_CONTYPEFK	Number		Key field (linking)
170	SKL	SKL_NAME	String	255	Key field (linking)
171	SKL	SKL_DESC	String	255	Key field (linking)
172	SKL	SKL_URL	String	255	Key field (linking)
173	SKL	SKL_LASTUPD	Date/Time		Key field (linking)
174	SKL	SKL_USERNAME	String	30	Key field (linking)
175	SKL	SKL_LCK	Number		Key field (linking)
176	TBLEMP	EMP_PK	Number		Event name (length is limiting)
177	TBLEMP	EMP_EMPCDFK	Number		Not used
178	TBLEMP	EMP_EMPSTATFK	Number		Not used
179	TBLEMP	EMP_MGREMPFK	Number		Event code (staff created)
180	TBLEMP	EMP_NO	String	25	Not used
181	TBLEMP	EMP_LNAME	String	35	Not used
182	TBLEMP	EMP_FNAME	String	35	Not used
183	TBLEMP	EMP_TITLE	String	5	Not used
184	TBLEMP	EMP_MI	String	1	Not used
185	TBLEMP	EMP_SUFFIX	String	5	Not used
186	TBLEMP	EMP_TTL	String	50	Not used
187	TBLEMP	EMP_STARTDT	Date/Time	8	Start date
188	TBLEMP	EMP_ENDDT	Date/Time	8	End date
189	TBLEMP	EMP_INTERNALIND	Number	2	Not used
190	TBLEMP	EMP_ADD1	String	50	Not used
191	TBLEMP	EMP_ADD2	String	50	Not used
192	TBLEMP	EMP_CTY	String	30	System generated
193	TBLEMP	EMP_STATE	String	2	System generated

Table 1 - Ingenium, Current System Data Fields (continued)

Item #	Table	Field	Type	Length	Comments
194	TBLEMP	EMP_CNTRY	String	35	System generated
195	TBLEMP	EMP_ZIP	String	10	Key field (linking)
196	TBLEMP	EMP_EMAIL	String	50	Key field (linking)
197	TBLEMP	EMP_PHN1	String	20	Key field (linking)
198	TBLEMP	EMP_PHN2	String	20	Key field (linking)
199	TBLEMP	EMP_FAX	String	20	Not used
200	TBLEMP	EMP_URL	String	255	Data entry date (system generated)
201	TBLEMP	EMP_NOTE	String	255	Date entry time (system generated)
202	TBLEMP	EMP_LSTUPD	Date/Time	8	Not used
203	TBLEMP	EMP_USERNAME	String	30	Not used
204	TBLEMP	EMP_LOC	Number		Not used
205	TBLEMPACOSKL	TBLEMPACOSKL_EMPFK	Number		Not used
206	TBLEMPACOSKL	TBLEMPACOSKL_SKLFK	Number		Not used
207	TBLEMPACOSKL	TBLEMPACOSKL_PROFFK	Number		Not used
208	TBLEMPACOSKL	TBLEMPACOSKL_FIRSTDT	Date/Time		Not used
209	TBLEMPACOSKL	TBLEMPACOSKL_LASTDT	Date/Time		Not used
210	TBLEMPACOSKL	TBLEMPACOSKL_NOTE	String		Not used
211	TBLEMPACOSKL	TBLEMPACOSKL_CERTNOTEDT	Date/Time		Not used
212	TBLEMPACOSKL	TBLEMPACOSKL_LASTUPD	Date/Time		Not used
213	TBLEMPACOSKL	TBLEMPACOSKL_USERNAME	String	30	Not used
214	TBLEMPACOSKL	TBLEMPACOSKL_LCK	Number		Not used
215	TBLEMPEVT	EMPEVT_PK	Number		Not used
216	TBLEMPEVT	EMPEVT_CHRGDORGFK	Number		Not used
217	TBLEMPEVT	EMPEVT_GRDFK	Number		Not used
218	TBLEMPEVT	EMPEVT_PAYTERMFK	Number		Course completion date
219	TBLEMPEVT	EMPEVT_MERGEDSKLIND	Number		Not used
220	TBLEMPEVT	EMPEVT_REGDT	Date/Time		Not used
221	TBLEMPEVT	EMPEVT_REGTM	Date/Time		System generated
222	TBLEMPEVT	EMPEVT_NOTE	String	255	System generated
223	TBLEMPEVT	EMPEVT_WAIVERIND	Number		System generated
224	TBLEMPEVT	EMPEVT_CNFMDDT	Date/Time		Not used
225	TBLEMPEVT	EMPEVT_CNCLDT	Date/Time		Not used
226	TBLEMPEVT	EMPEVT_CNCLTM	Date/Time		Not used
227	TBLEMPEVT	EMPEVT_PAIDDT	Date/Time		Not used
228	TBLEMPEVT	EMPEVT_PAIDTM	Date/Time		Key field (linking)
229	TBLEMPEVT	EMPEVT_REIMBIND	Number		Grade -needs length of 1
230	TBLEMPEVT	EMPEVT_TRVLCOST	Number		System generated
231	TBLEMPEVT	EMPEVT_BILLEDDT	Date/Time		System generated
232	TBLEMPEVT	EMPEVT_OTHERCOST	Number		System generated
233	TBLEMPEVT	EMPEVT_CNFMIND	Number		Not used
234	TBLEMPEVT	EMPEVT_RMNDNOTEDT	Date/Time		Key field (linking)
235	TBLEMPEVT	EMPEVT_CNFMNOTEDT	Date/Time		Key field (linking)
236	TBLEMPEVT	EMPEVT_CNCLNOTEDT	Date/Time		Key field (linking)
237	TBLEMPEVT	EMPEVT_ACTUALCOST	Number		DCIS staff name
238	TBLEMPEVT	EMPEVT_CMPLTDT	Date/Time		Assigned username
239	TBLEMPEVT	EMPEVT_CERTNOTEDT	Date/Time		Not used
240	TBLEMPEVT	EMPEVT_REIMBAMT	Number		Not used
241	TBLEMPEVT	EMPEVT_LASTUPD	Date/Time		System generated
242	TBLEMPEVT	EMPEVT_USERNAME	String	50	System generated

Table 1 - Ingenium, Current System Data Fields (continued)

Item #	Table	Field	Type	Length	Comments
243	TBLEMPEVT	EMPEVT_LCK	Number		System generated
244	TBLEMPEVT	EMPEVT_PCTGRD	Number		Key field (linking)
245	TBLEMPEVT	EMPEVT_ELAPSEDMINUTES	Number		Key field (linking)
246	TBLEMPEVT	EMPEVT_FIRSTLAUNCHDT	Date/Time		Instructor SSN
247	TBLEMPEVT	EMPEVT_FIRSTLAUNCHTM	Date/Time		"Position" field
248	TBLEMPIJOB	EMPIJOB_EMPFK	Number		SGP instructor last name
249	TBLEMPIJOB	EMPIJOB_JOBFK	Number		SGP instructor first name
250	TBLEMPIJOB	EMPIJOB_PRMVIND	Number		Mr., Mrs.
251	TBLEMPIJOB	EMPIJOB_NOTE	String	255	Instructor middle initial
252	TBLEMPIJOB	EMPIJOB_LSTUPD	Date/Time	8	Instructor Jr, Sr
253	TBLEMPIJOB	EMPIJOB_USRNAME	String	20	Not used
254	TBLEMPIJOB	EMPIJOB_LOC	Number		Instructor address
255	TBLEMPIORG	EMPORG_EMPFK	Number		Instructor address
256	TBLEMPIORG	EMPORG_ORGFK	Number		Not used
257	TBLEMPIORG	EMPORG_PRMVIND	Number	2	Instructor city
258	TBLEMPIORG	EMPORG_LSTUPD	Date/Time	8	Instructor state
259	TBLEMPIORG	EMPORG_USRNAME	String	30	Instructor county
260	TBLEMPIORG	EMPORG_LCK	Number		Instructor postal code
261	TBLOPTEMP	OPTEMP_FK	Number		Instructor email
262	TBLOPTEMP	OPTEMP_TXT1	String	255	Instructor telephone
263	TBLOPTEMP	OPTEMP_TXT2	String	255	Instructor telephone 2
264	TBLOPTEMP	OPTEMP_TXT3	String	255	Instructor facsimile
265	TBLOPTEMP	OPTORG_TXT4	String	255	Not used
266	TBLOPTEMP	OPTORG_MEM01	String	2000	Free text notes
267	TBLOPTEMP	OPTEMP_DT1	Date/Time		System generated
268	TBLOPTEMP	OPTEMP_DT2	Date/Time		System generated
269	TBLOPTEMP	OPTEMP_IND1	Number		System generated
270	TBLOPTEMP	OPTEMP_MONEY	Number		Key field (linking)
271	TBLOPTEMP	OPTEMP_INT1	Number		Date of birth
272	TBLOPTEMP	OPTEMP_FLOAT1	Number		Gender
273	TBLOPTEMP	OPTEMP_OLE1	OLE		Firearms initial certification date
274	TBLOPTEMP	OPTEMP_LSTUPD	Date/Time		Firearms recertification date
275	TBLOPTEMP	OPTEMP_USRNAME	String	30	Free text notes
276	TBLOPTEMP	OPTEMP_LCK	Number		General topics cert date
277	TBLOPTORG	OPTORG_EMPFK	Number		General topics recent date
278	TBLOPTORG	OPTORG_ORGFK	Number		Active/inactive
279	TBLOPTORG	OPTORG_TXT1	String	255	Not used
280	TBLOPTORG	OPTORG_TXT2	String	255	
281	TBLOPTORG	OPTORG_TXT3	String	255	not used
282	TBLOPTORG	OPTORG_TXT4	String	255	
283	TBLOPTORG	OPTORG_MEM01	String	255	System generated
284	TBLOPTORG	OPTORG_DT1	Date/Time		System generated
285	TBLOPTORG	OPTORG_DT2	Date/Time		System generated
286	TBLOPTORG	OPTORG_IND1	Number		Key field (linking)
287	TBLOPTORG	OPTORG_MONEY	Number		Key field (linking)
288	TBLOPTORG	OPTORG_INT1	Number		Specialized skill name for non-cert instructors
289	TBLOPTORG	OPTORG_FLOAT1	Number		Not used
290	TBLOPTORG	OPTORG_OLE1	OLE		Not used
291	TBLOPTORG	OPTORG_LSTUPD	Date/Time		System generated

Table 1 - Ingenium, Current System Data Fields (continued)

Item #	Table	Field	Type	Length	Comments
292	TBLOPTORG	OPTORG_USRNAME	String	30	System generated
293	TBLOPTORG	OPTORG_LCK	Number		System generated
294	USR	USR_PK	Number		Key field (linking)
295	USR	USR_EMPFK	Number		Key field (linking)
296	USR	USR_ROLEFK	Number		Key field (linking)
297	USR	USR_NAME	String	255	Not used
298	USR	USR_USRNAME	String	30	Not used
299	USR	USR_VIEWALLEMPSSIND	Number		Not used
300	USR	USR_STATUS	Number		Not used
301	USR	USR_LASTUPD	Date/Time		System generated
302	USR	USR_USRNAME	String	30	System generated
303	USR	USR_LCK	Number		System generated
304	VEN	VEN_PK	Number		Key field (linking)
305	VEN	VEN_NAME	String	50	Key field (linking)
306	VEN	VEN_TTL	String	50	System generated
307	VEN	VEN_PRIND	Number		System generated
308	VEN	VEN_FNAME	String	35	System generated
309	VEN	VEN_LNAME	String	35	Key field (linking)
310	VEN	VEN_ADD1	String	50	State hierarchy (=New York State)
311	VEN	VEN_ADD2	String	50	System generated
312	VEN	VEN_CITY	String	30	System generated
313	VEN	VEN_STATE	String	2	System generated
314	VEN	VEN_ZIP	String	10	Key field (linking)
315	VEN	VEN_CNTRY	String	35	Key field (linking)
316	VEN	VEN_EMAIL	String	50	Key field (linking)
317	VEN	VEN_PHN1	String	20	Primary employer
318	VEN	VEN_PHN2	String	20	Employee start date
319	VEN	VEN_FAX	String	20	Employee end date
320	VEN	VEN_URL	String	255	Employee CPL designation and title (literal)
321	VEN	VEN_NOTE	String	255	Key field (linking)
322	VEN	VEN_LSTUPD	Date/Time	8	System generated
323	VEN	VEN_USRNAME	String	30	System generated
324	VEN	VEN_LCK	Number		System generated

This Page Intentionally Blank

Appendix H

Contract Award Protest Procedure

Intentionally Blank

CONTRACT AWARD PROTEST PROCEDURE FOR CONTRACTS AWARDED BY THE DIVISION OF CRIMINAL JUSTICE SERVICES

Section 1 Applicability
Section 2 Definitions
Section 3 General Requirements
Section 4 Protest Procedure
Section 5 Appeals

1. Applicability

Consistent with the provisions of the Procurement Lobbying Law (State Finance Law §139-j), it is the policy of the Division of Criminal Justice Services (DCJS) to identify a sole Procurement Contact to receive all inquiries during an identified procurement period. DCJS will attempt to resolve inquiries submitted to the identified sole Procurement Contact, and will advise parties initiating such inquiries of the existence of this formal protest policy should the informal process fail to resolve the matter. **Final agency determinations or recommendations for award will not be reconsidered by DCJS unless a formal written protest is timely filed according to the procedures specified below. The procedures below must be used** which set forth the procedure to be utilized when an interested party challenges a contract award by DCJS. These guidelines apply to all contract awards by DCJS, including sole source procurements, single source procurements, emergency procurements and procurements awarded after a mini-bid process.

2. Definitions

- (a) "Offerer" mean an individual or entity who has submitted an offer in response to a solicitation for commodities or services issued by DCJS.
- (b) "Responsive Offerer" means a bidder or Offerer meeting all of the minimum specifications and requirements as prescribed in a solicitation for commodities or services by DCJS.
- (c) "Successful Offerer" means the responsive bidder or Offerer which receives written notification from DCJS indicating that its bid or offer has been accepted.
- (d) "Interested party" means a participant in the procurement process and those who would be bona fide participants but whose participation in the procurement process has been foreclosed by the actions of DCJS.
- (e) "Contract award" is a written determination from DCJS to an Offerer indicating that the DCJS has accepted its bid or offer (see State Finance Law §163[10][a]).
- (f) "Emergency" means an urgent and unexpected requirement where health and public safety or the conservation of public resources is at risk (see State Finance Law §163[1] [b]).

(g) “Mini-bid process” is an abbreviated bid and selection process for individual agency projects utilizing a list of prequalified vendors on a back drop contract.

(h) “Back drop contract” means a contract consisting of a pool of prequalified vendors who are eligible to participate in a secondary mini-bid award process, or other specified selection process.

(i) “Single source” means a procurement in which although two or more Offerers can supply the required commodities or services, DCJS, upon written findings setting forth the material and substantial reasons therefor, awards the contract to one Offerer over the other (see State Finance Law §163[1][h]).

(j) “Sole source” means a procurement in which only one Offerer is capable of supplying the required commodities or services (see, State Finance Law §163[1] [g]).

(k) “Protest” means a written challenge to a contract award by DCJS.

(l) “Comptroller” means the Comptroller of the State of New York, as well as his or her designee.

(m) “Commissioner” means the Commissioner of the Division of Criminal Justice Services, an agency of the State of New York, as well as his or her designee.

3. General Requirements

(a) Any solicitation issued by DCJS with respect to a contract award subject to these guidelines, including an Invitation for Bid, a Request for Proposal, or other similar document, shall provide notice that any interested party may protest the contract award. Such notice shall indicate that a protest of a contract award is to be filed with the DCJS Director of Financial Administration at:

Ms. Kim Szady
Director, Financial Administration
New York State Division of Criminal Justice Services
Alfred E. Smith Office Building
80 South Swan Street, 10th Floor
Albany, NY 12210

The solicitation must include a copy of these guidelines, or advise Offerers that a copy of these guidelines will be provided to the Offerer upon request.

(b) All Offerers shall be given written notice of the contract award or of a proposed award. Any unsuccessful Offerer, upon request, must be afforded an opportunity for a debriefing at least five business days prior to the date by which any protest must be filed. Notwithstanding the foregoing, in any case where DCJS has reduced the time period for the filing of a protest in accordance with section 4(a) of these guidelines, DCJS shall provide in the solicitation for a reasonable and appropriate method to debrief the Offerers in a timely manner. An Offerer's failure to request a debriefing in a timely fashion shall not cause an extension of the time period within which a protest must be filed.

(c) A protest must be in writing and must contain specific factual and/or legal allegations setting forth the basis on which the protesting party challenges the contract award by the DCJS. A formal protest must include:

- (i) a statement of all legal and/or factual grounds for disagreement with a DCJS specification or purchasing determination;
- (ii) a description of all remedies or relief requested; and
- (iii) copies of all applicable supporting documentation

(d) Any interested party will be given the opportunity to participate in the protest procedure.

(e) The DCJS Director of Financial Administration may, in his or her sole discretion, waive any deadline or requirement set forth in these guidelines, or consider any materials, submitted in writing, beyond the time periods set forth in these guidelines.

(f) Where the DCJS Director of Financial Administration deems appropriate, the DCJS Director of Financial Administration may require the protesting party, the procuring Division of DCJS, DCJS staff involved in the procurement, the successful Offerer, or any other interested party, to address and/or submit further information with respect to additional issues raised by the DCJS Director of Financial Administration review of the procurement.

(g) Nothing herein shall preclude the DCJS Director of Financial Administration from obtaining information relevant to the procurement from any other source, as he or she deems appropriate.

4. Protest Procedure

(a) Any interested party may file a protest with the DCJS Director of Financial Administration within ten business days from the date of the notice by DCJS of the contract award, except that:

- (i) any protest concerning the terms and conditions of the solicitation or other matters that would be apparent to an interested party prior to the date set in the solicitation for the receipt of bids including but not limited to matters concerning errors, omissions or prejudice in the bid specifications or documents must be filed on or before the date set in the solicitation for the receipt of bids or proposals; and

(ii) where DCJS determines that sufficient circumstances exist DCJS may set forth a different time period for filing protests in the solicitation.

Any filing deadlines may be waived by the DCJS Director of Financial Administration pursuant to section 3(e) of these guidelines. A formal protest must be submitted in writing to DCJS, by surface mail addressed to the DCJS Director of Financial Administration pursuant to section 3(a) above, or, where permitted in the solicitation, by facsimile or e-mail transmission. The following statement must be clearly and prominently displayed on the envelope or package or header of electronic or facsimile transmittal: "Bid Protest of DCJS Solicitation (CJS 2014- 01)".

(b) The DCJS Director of Financial Administration shall refer any protest either to an individual employee or group of employees of DCJS, or to an independent hearing officer who is not an employee of DCJS. The decision regarding to whom the bid protests is referred shall be in the sole discretion of the DCJS Director of Financial Administration. Where the protest is referred to a DCJS employee or a group of DCJS employees, no such employee may have been actively involved in the procurement process being protested.

(c) The DCJS Director of Financial Administration will provide a copy of any protest filed to the successful Offerer.

(d) The DCJS Director of Financial Administration may summarily deny a protest that fails to contain specific factual or legal allegations, or raises only issues of law that have already been decided by the Courts or by the Comptroller of the State of New York.

(e) Except where the DCJS Director of Financial Administration summarily denies the protest, the procuring Division of DCJS shall file an answer to the protest within seven business days of the filing of the protest. The answer to the protest should address all the factual and legal allegations contained in the protest. A copy of the answer filed by the procuring Division of DCJS shall be delivered to the protester and the successful Offerer. The successful Offerer may, but shall not be required to, file an answer to the protest. Any answer by the successful Offerer must be filed with the DCJS Director of Financial Administration no later than the date that the procuring Division of DCJS is required to file its answer. If the successful Offerer chooses to file an answer, it must deliver a copy of such answer to the procuring Officer of DCJS and the protester, and its answer must contain an affirmation as to such delivery.

(f) The protesting party may, but is not required to, file a reply to the answer of the procuring Division of DCJS and the successful Offerer. Such reply shall be filed with the DCJS Director of Financial Administration no later than five business days after the date that the procuring Division of DCJS answer is filed. A copy of such reply shall also be delivered to the successful Offerer, and the protester's reply must contain an affirmation as to such delivery.

(g) Upon the DCJS Director of Financial Administration's own initiative, or upon request of any participant in the protest process, the DCJS Director of Financial Administration may in his or her sole discretion act on an expedited basis, upon written notification to the interested parties, in which case the DCJS Director of Financial Administration will advise all participants of filing deadlines.

(h) During the time period in which a protest may be filed, or during the resolution of a pending protest, DCJS may negotiate terms and conditions of the contract with the successful Offerer. However, a contract will not be approved by the Office of the State Comptroller Bureau of Contracts before the expiration of the time period for filing a protest, or, if a protest has been filed, before the resolution of the protest.

(i) The person or persons designated by the DCJS Director of Financial Administration to consider the protest shall review all of the filings submitted by the parties, and the procurement record, and shall prepare a written recommendation to the DCJS Director of Financial Administration, or his or her designee, addressing all of the issues that have been raised by the protest.

(j) The person or persons designated by the DCJS Director of Financial Administration to consider the protest shall determine whether, in addition to the review of the filings submitted by the parties and the procurement record, it is necessary to conduct a fact finding hearing. The person or persons so designated shall decide the level of formality of such a hearing.

(k) The DCJS Director of Financial Administration, or his or her designee, may accept, modify or reject such recommendation.

(l) In making his or her determination with regard to the protest, the DCJS Director of Financial Administration, or his or her designee, may, in his or her sole discretion, consider any additional material and relevant information from any source relating to the allegations set forth in the protest.

(m) All parties that have participated in the protest, as well as the original successful Offerer, shall be provided with a copy of the final determination of the DCJS Director of Financial Administration or his or her designee. The determination shall be made part of the procurement record.

5. Appeals

(a) The protest determination of the DCJS Director of Financial Administration shall be deemed a final and conclusive agency determination unless a written notice of appeal is received no more than five business days after the date the final protest decision is sent to the Offerer. Such notice of appeal must be filed in writing at the address set forth below:

**Commissioner
New York State Division of Criminal Justice Services
Reference: Bid Protest of DCJS Solicitation (CJS 2014- 01)
Alfred E. Smith Office Building
80 South Swan Street, 10th Floor
Albany, NY 12210**

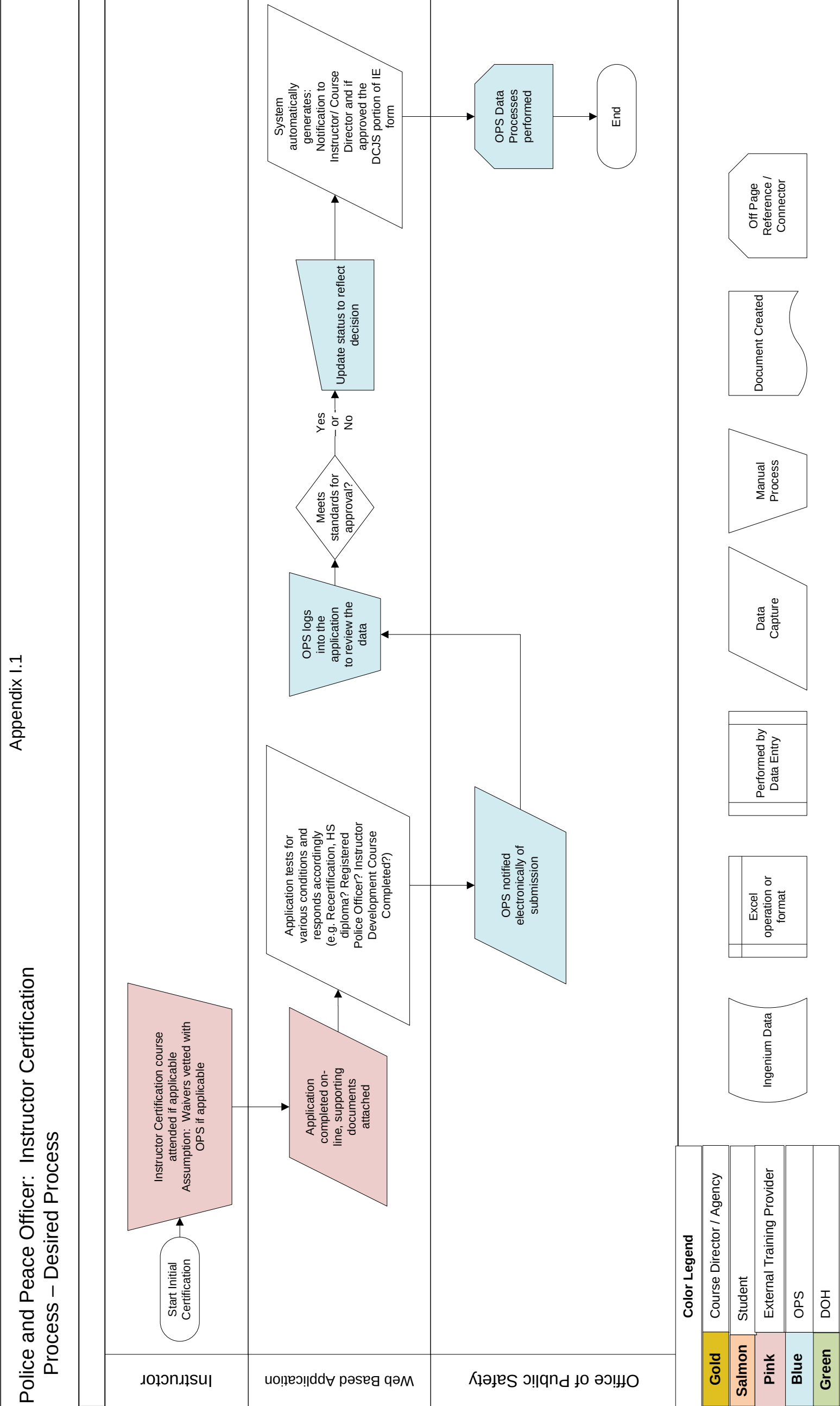
(b) The Commissioner shall hear and make a final written determination on all appeals within ten business days of the date the Appeal is received. The Commissioner may designate a person or persons to act on his or her behalf.

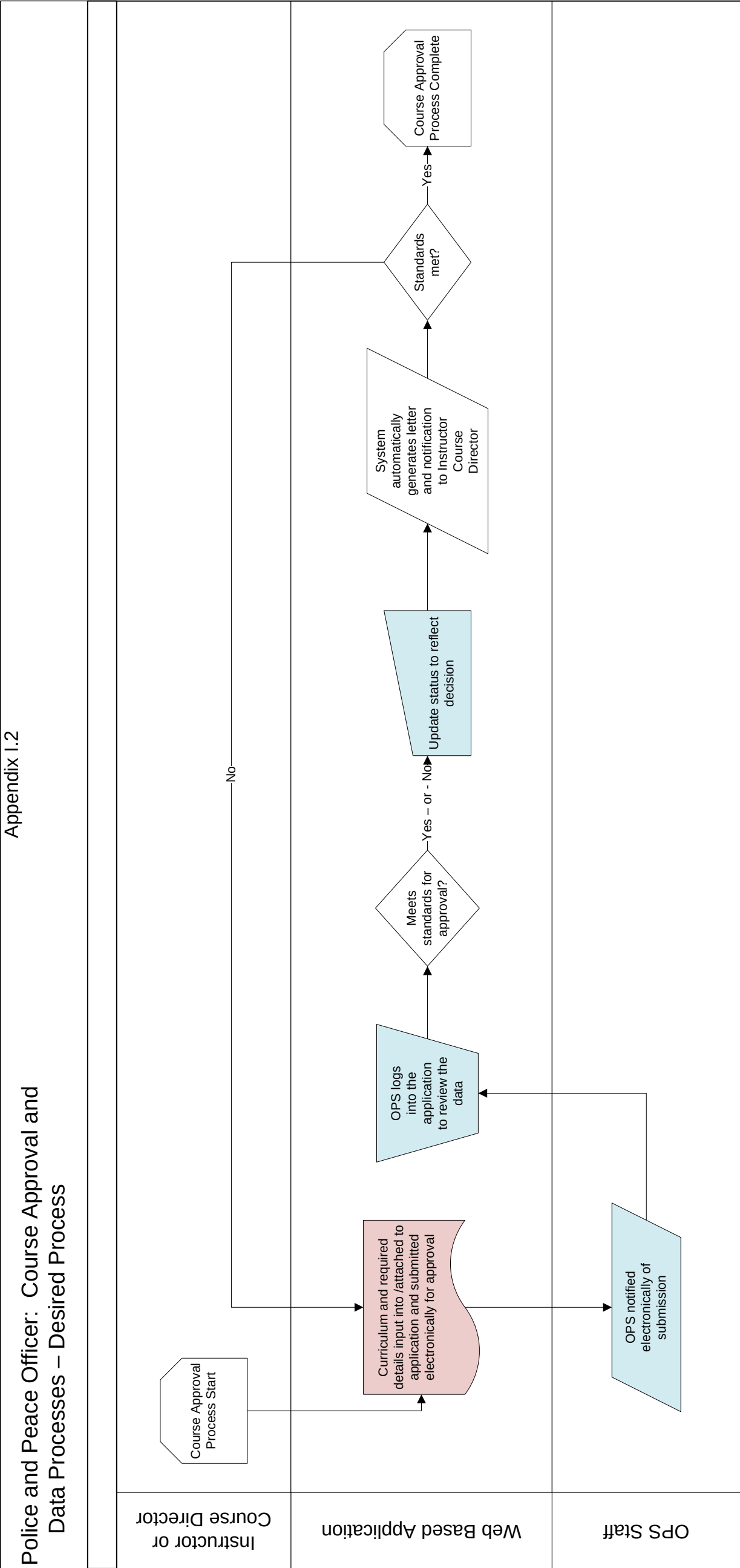
(c) A formal protest appeal may not introduce new facts unless responding to issues newly raised as a result of the final protest determination.

Appendix I

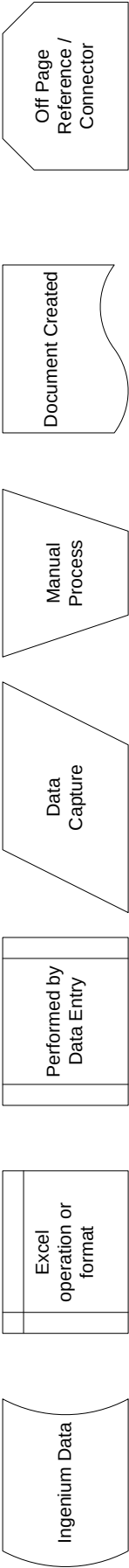
Key Process Flow Charts

Intentionally Blank

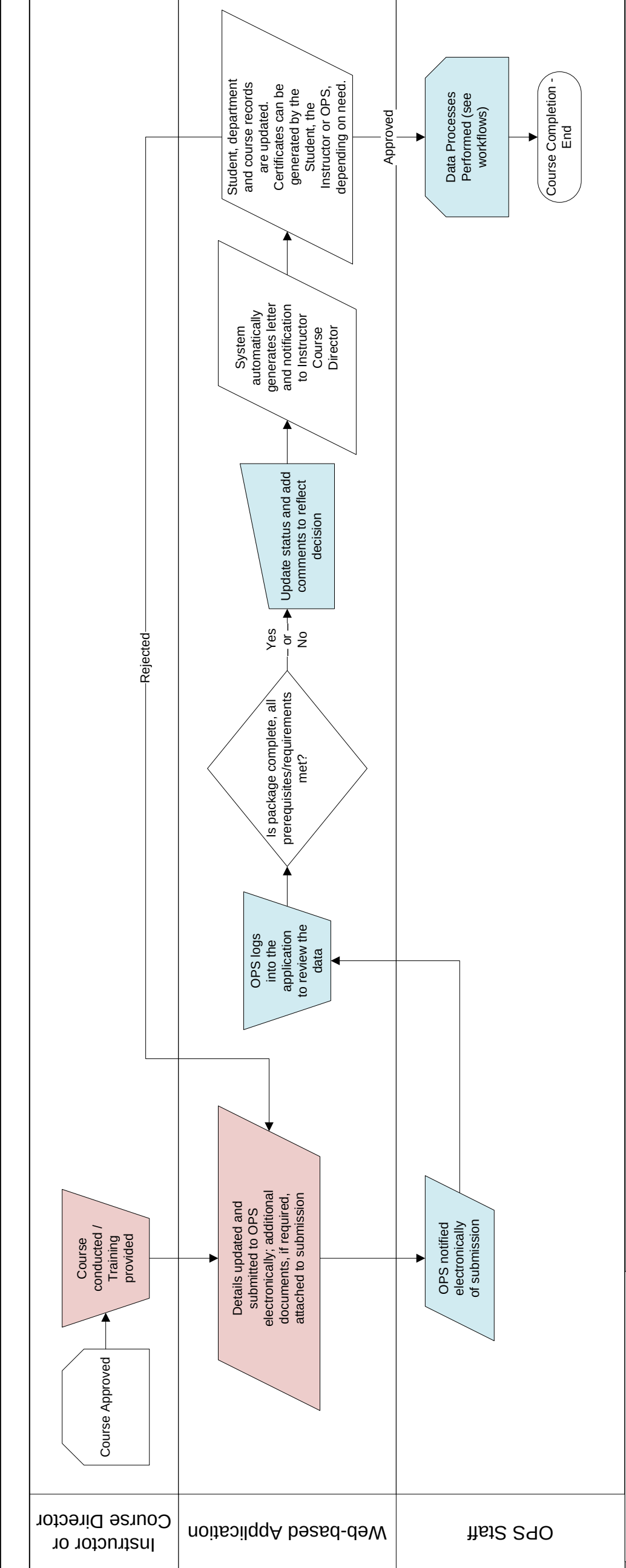




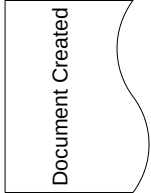
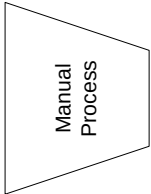
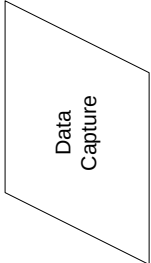
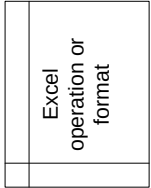
Color Legend	
Gold	Course Director / Agency
Salmon	Student
Pink	External Training Provider
Blue	OPS
Green	DOH

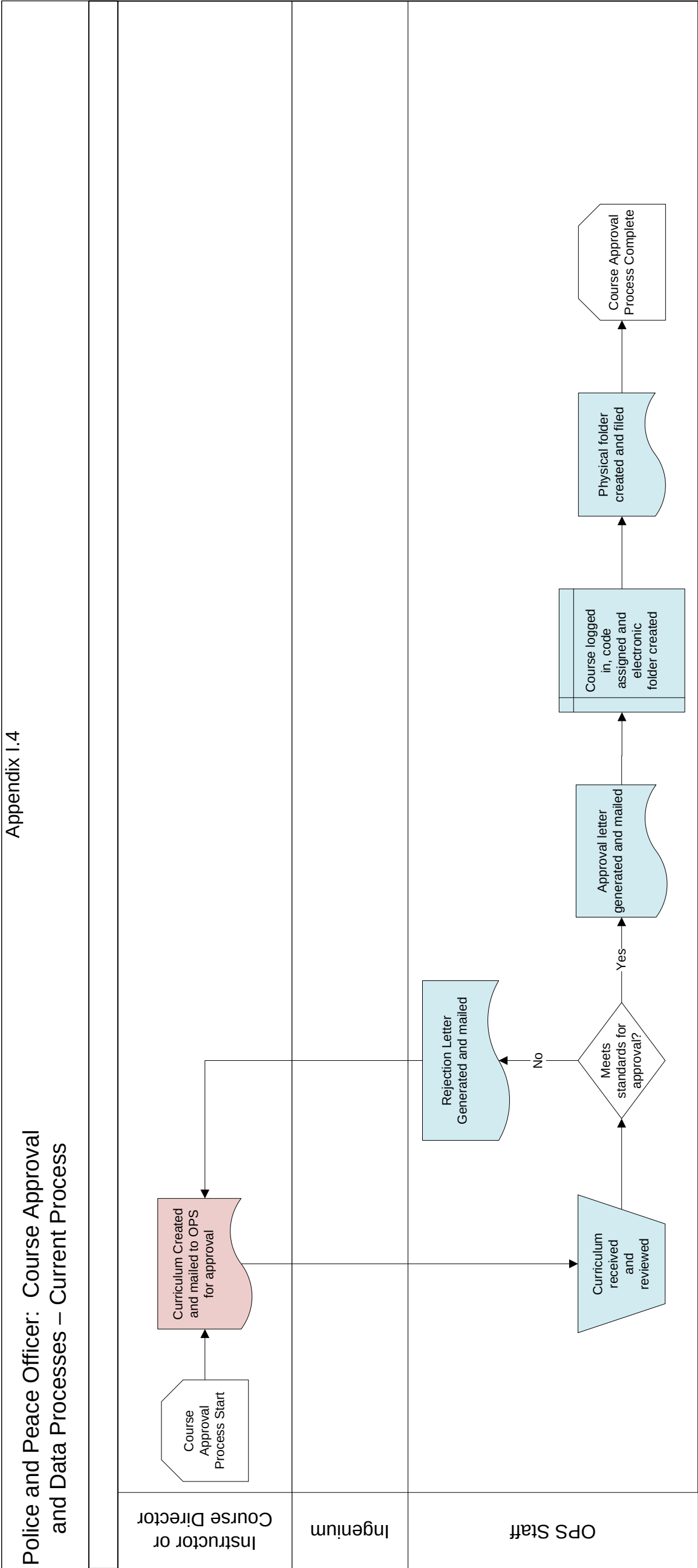


Police and Peace Officer: Course Completion and Data Processes – Desired Process

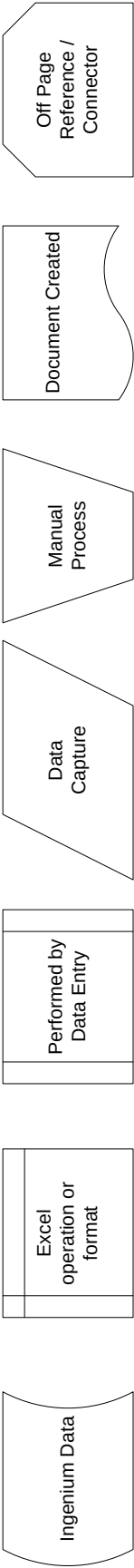


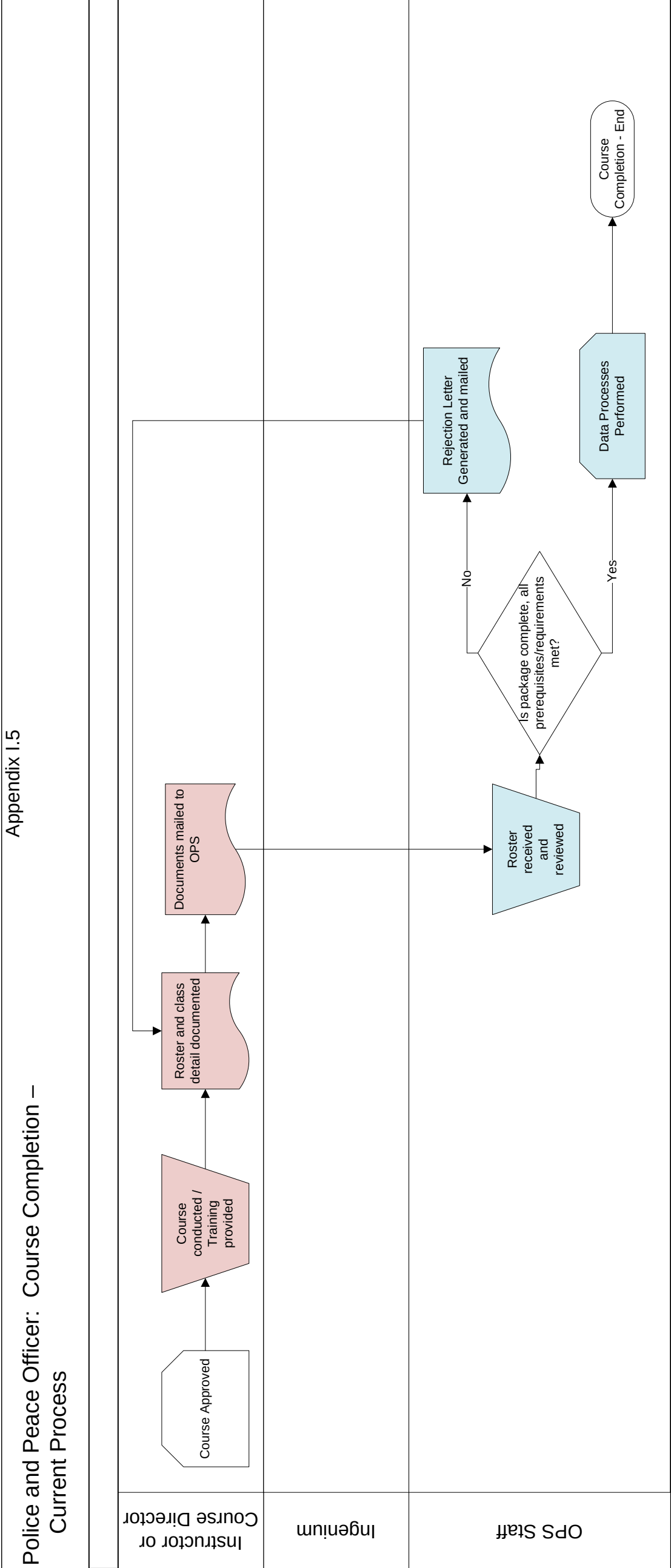
Color Legend	
Gold	Course Director / Agency
Salmon	Student
Pink	External Training Provider
Blue	OPS
Green	DOH



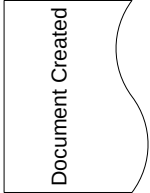
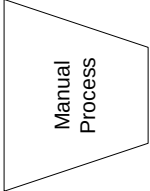
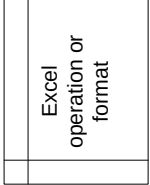


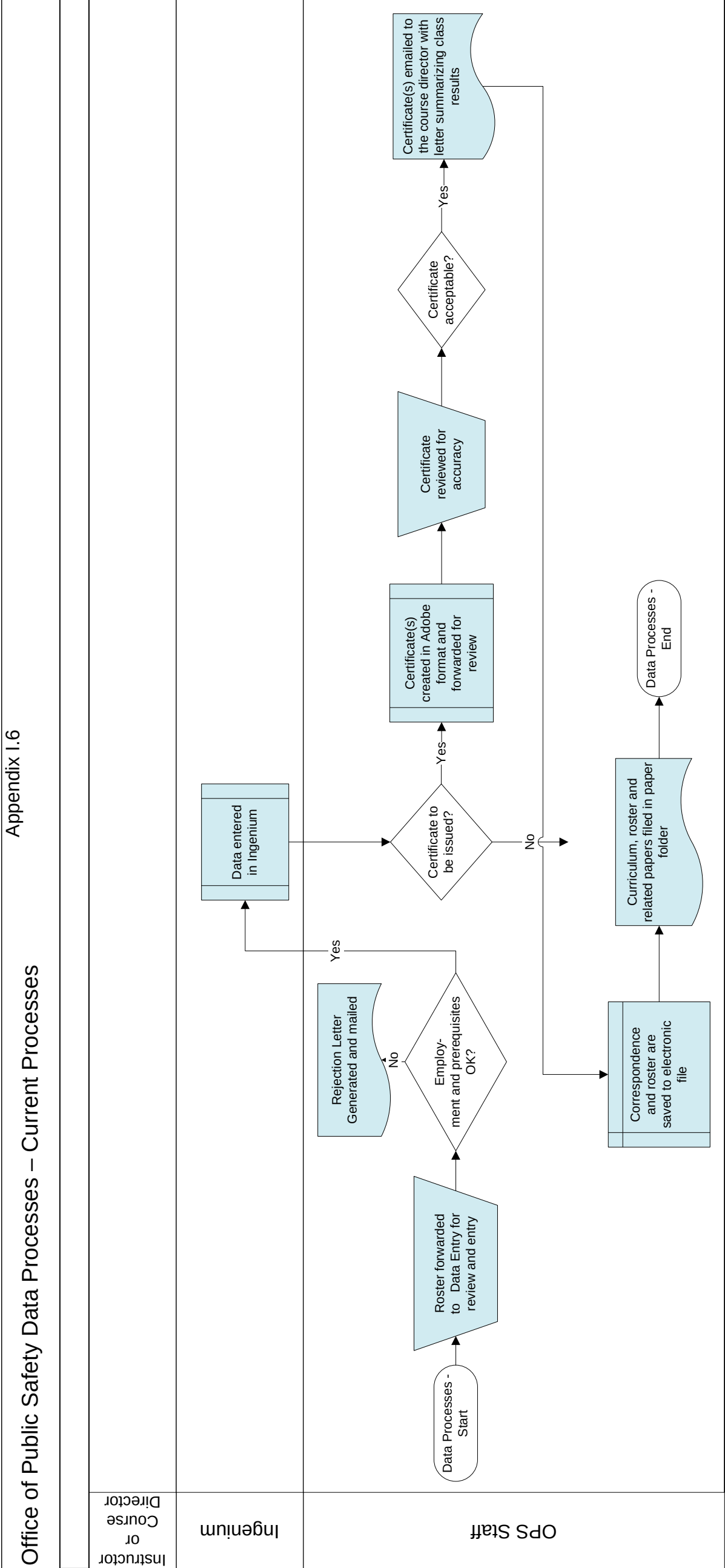
Color Legend	
Gold	Course Director / Agency
Salmon	Student
Pink	External Training Provider
Blue	OPS
Green	DOH



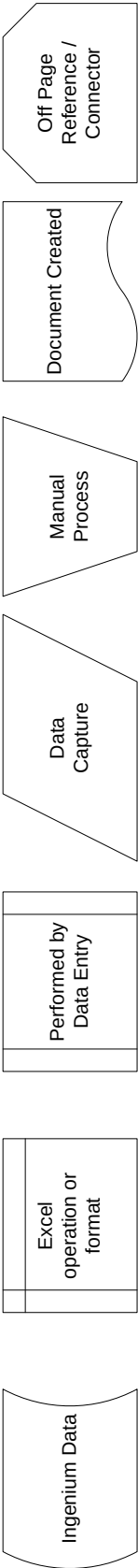


Color Legend	
Gold	Course Director / Agency
Salmon	Student
Pink	External Training Provider
Blue	OPS
Green	DOH

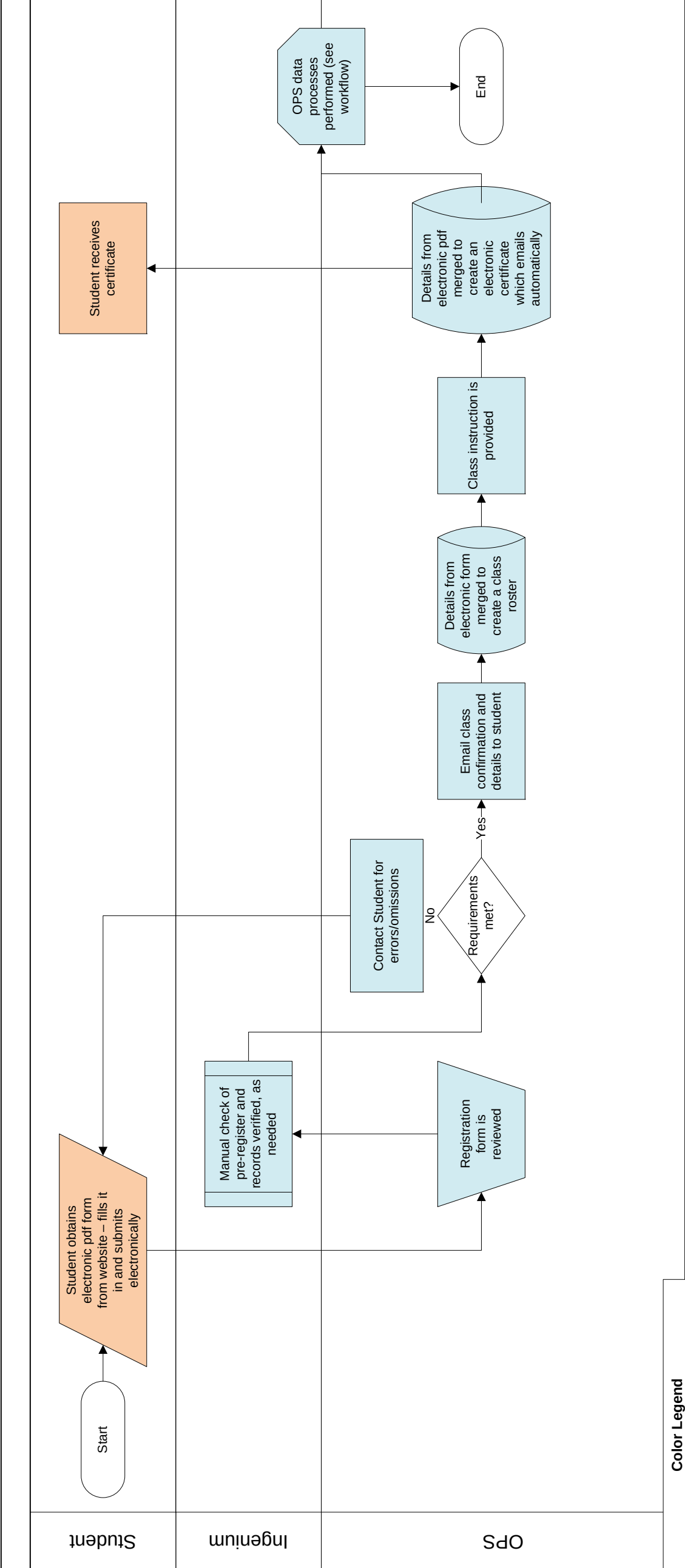




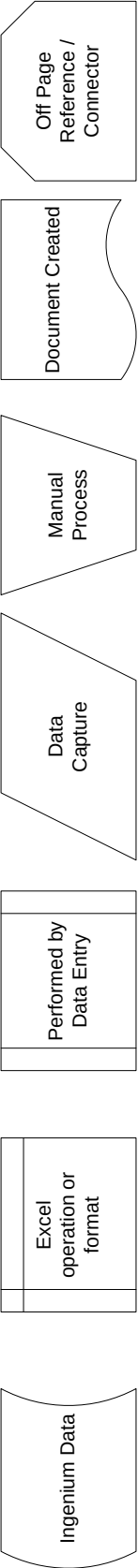
Color Legend	
Gold	Course Director / Agency
Salmon	Student
Pink	External Training Provider
Blue	OPS
Green	DOH

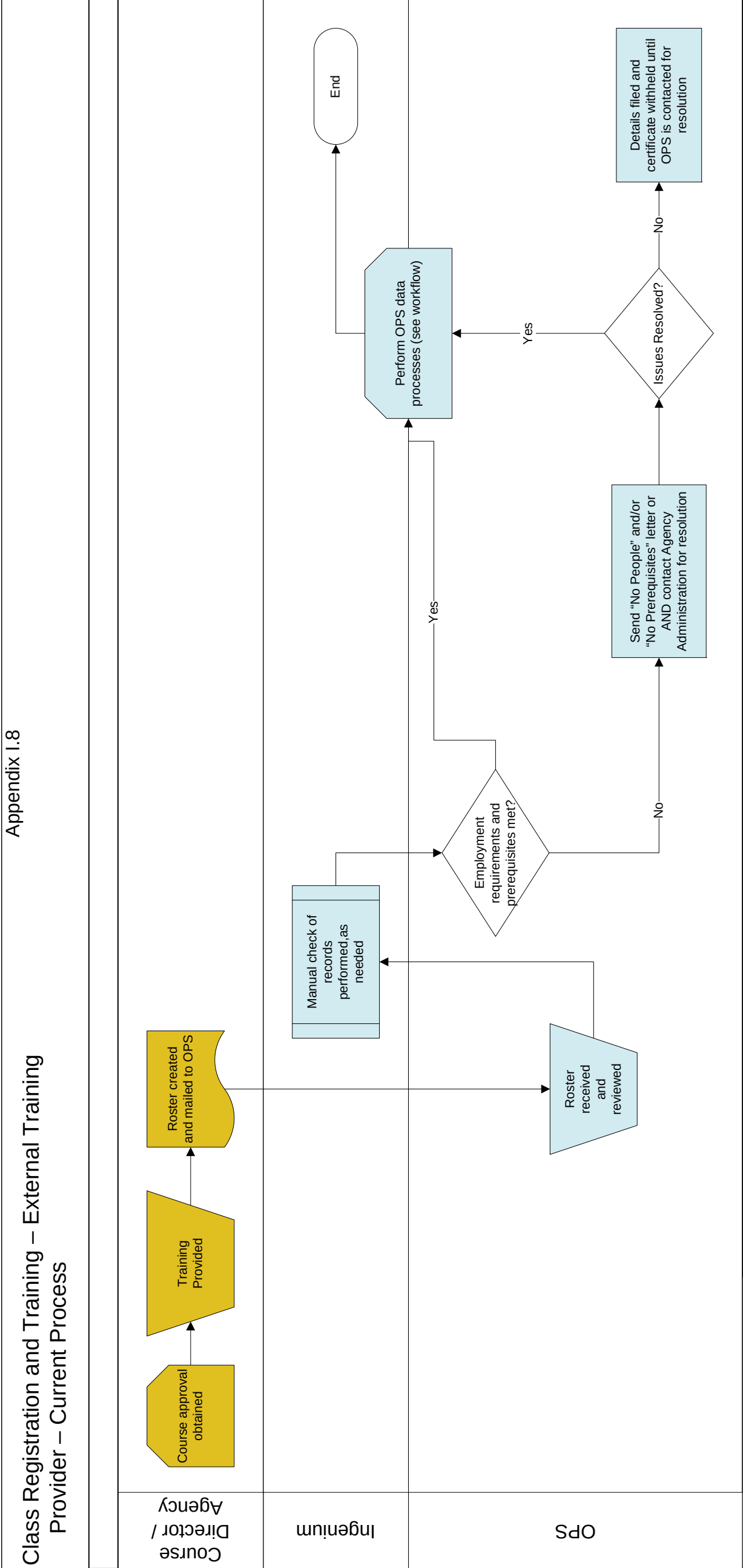


Class Registration and Training – OPS Provided Training –
Current Process

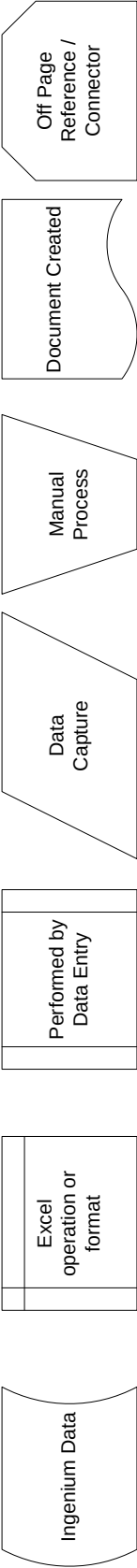


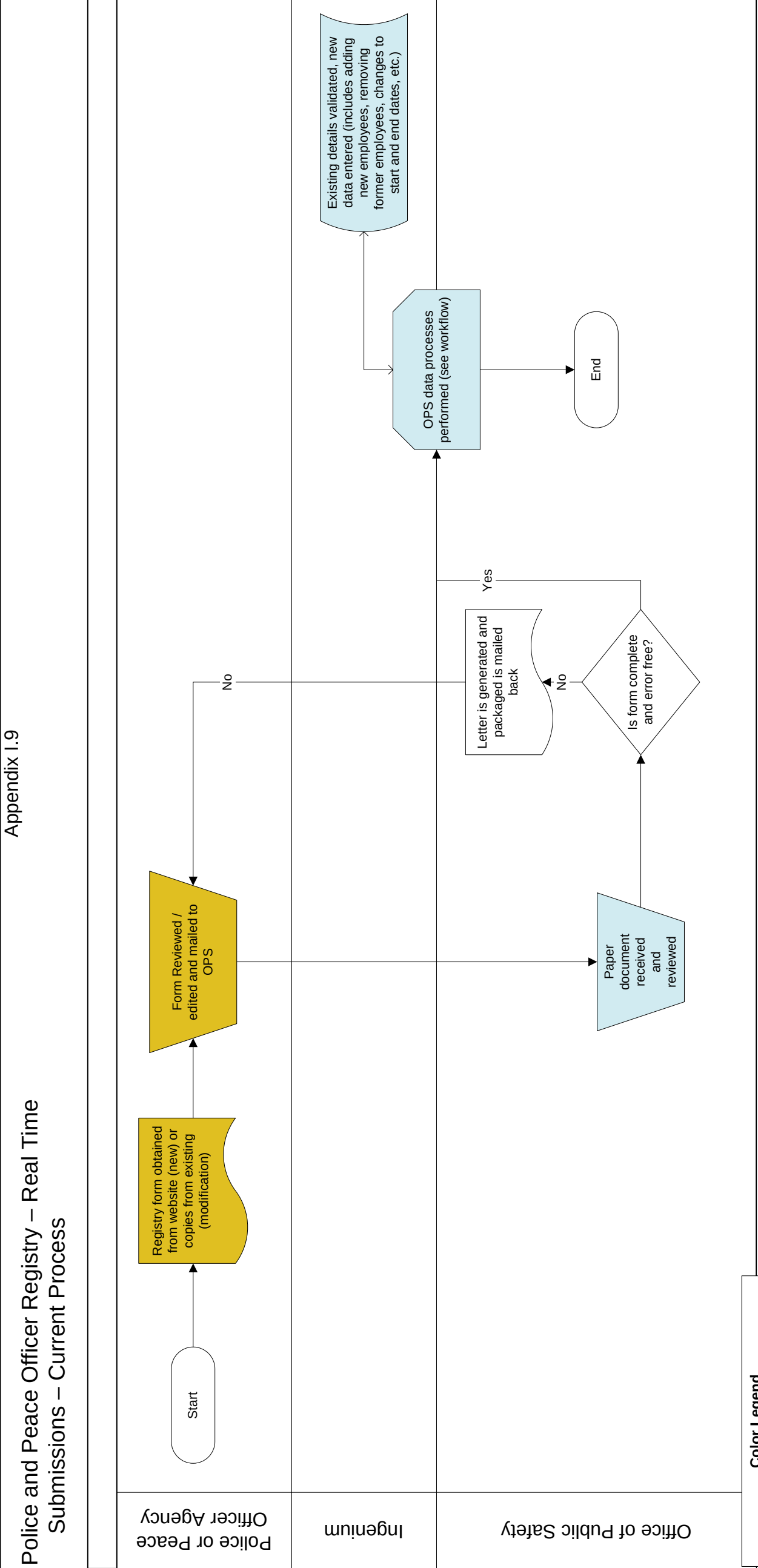
Color Legend	
Gold	Course Director / Agency
Salmon	Student
Pink	External Training Provider
Blue	OPS
Green	DOH



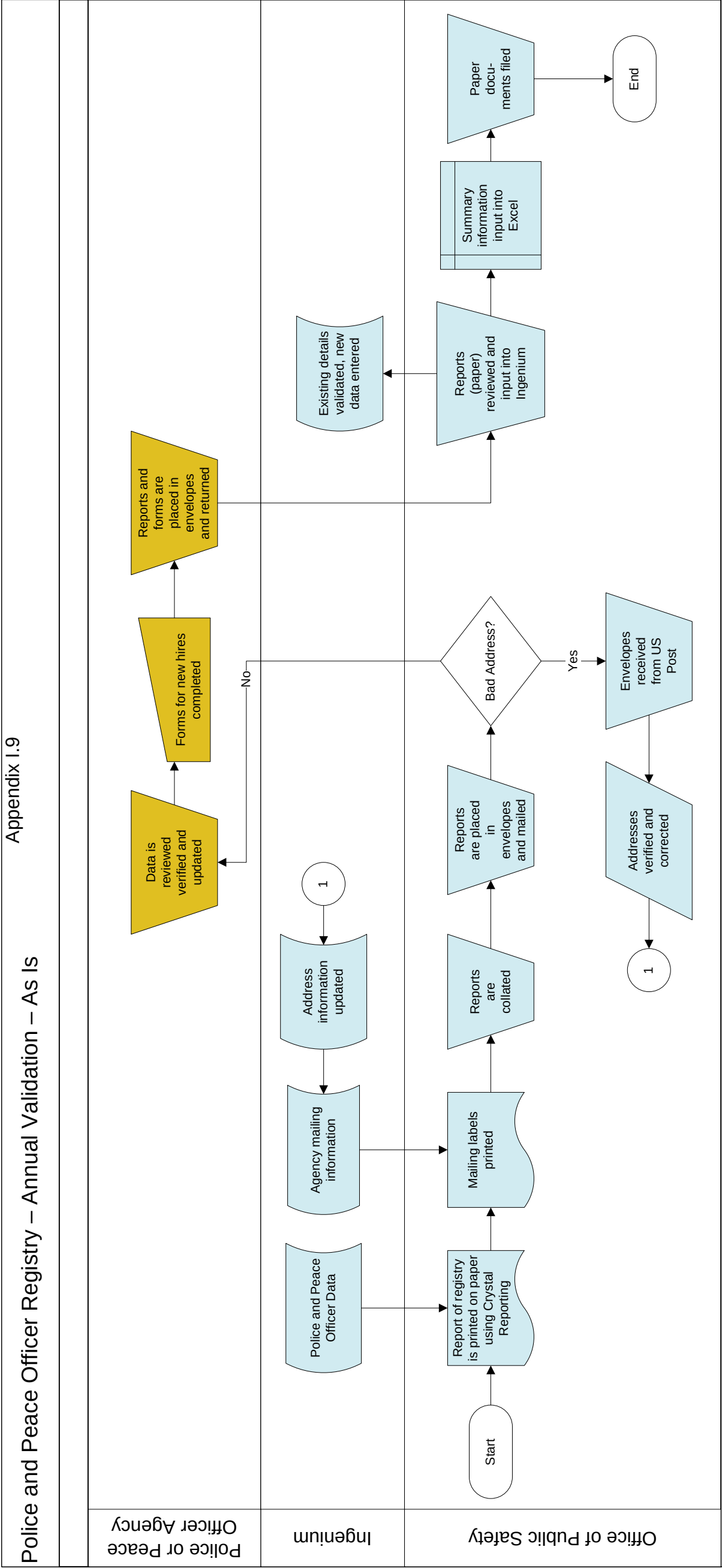


Color Legend	
Gold	Course Director / Agency
Salmon	Student
Pink	External Training Provider
Blue	OPS
Green	DOH

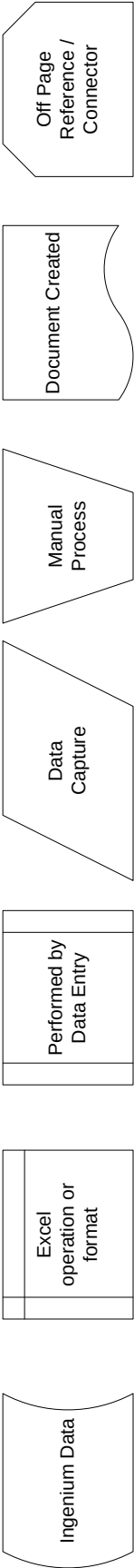


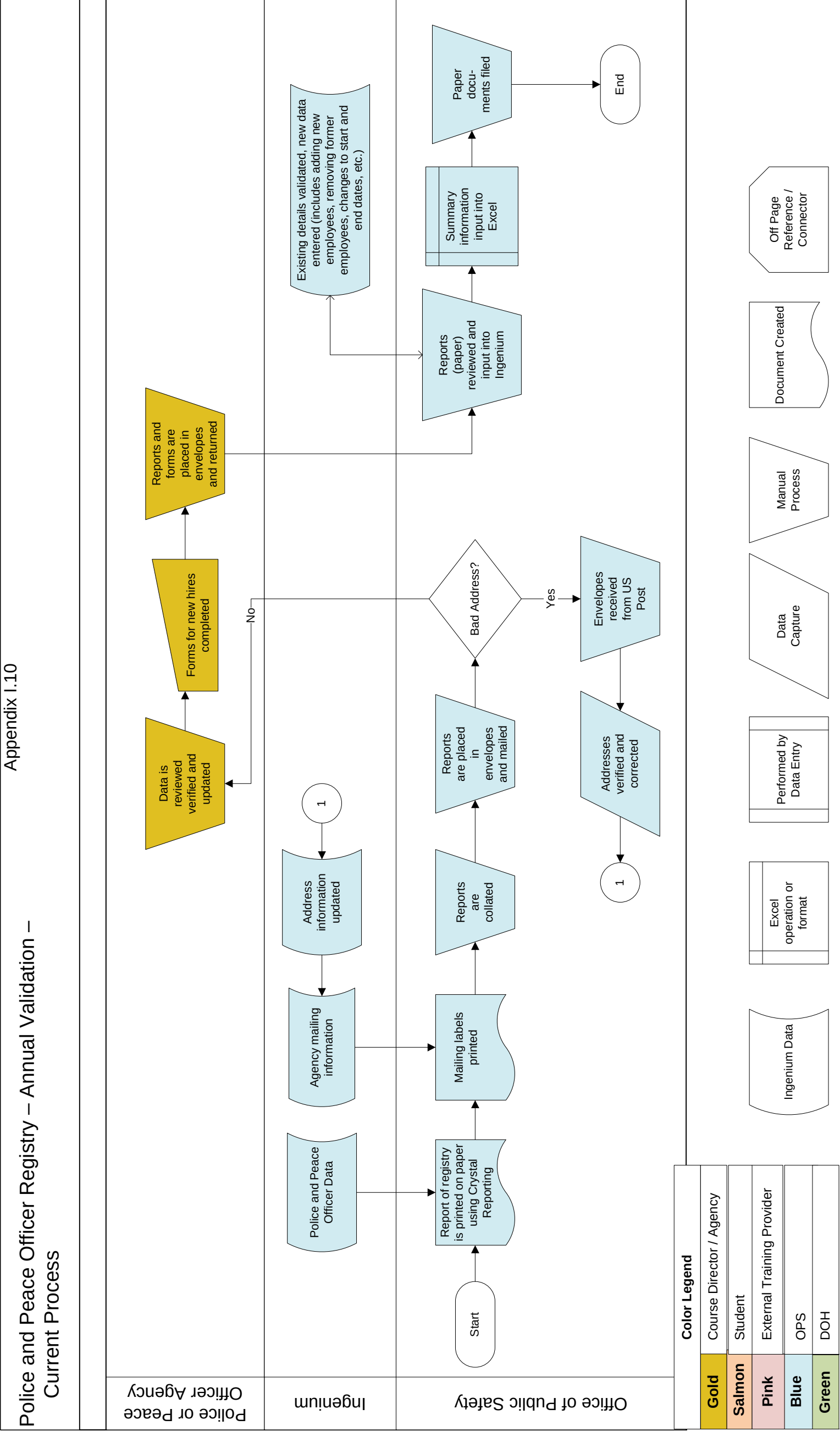


Color Legend	
Gold	Course Director / Agency
Salmon	Student
Pink	External Training Provider
Blue	OPS
Green	DOH

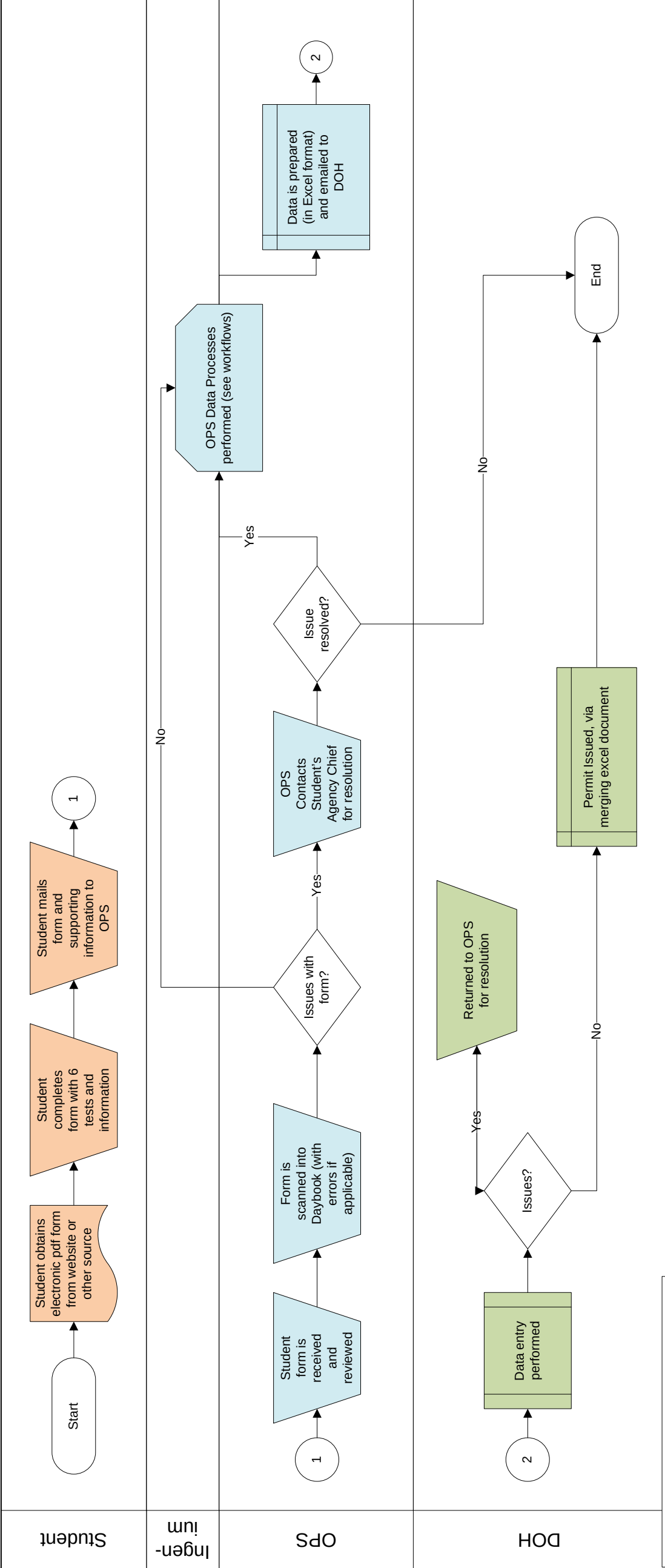


Color Legend	
Gold	Course Director / Agency
Salmon	Student
Pink	External Training Provider
Blue	OPS
Green	DOH



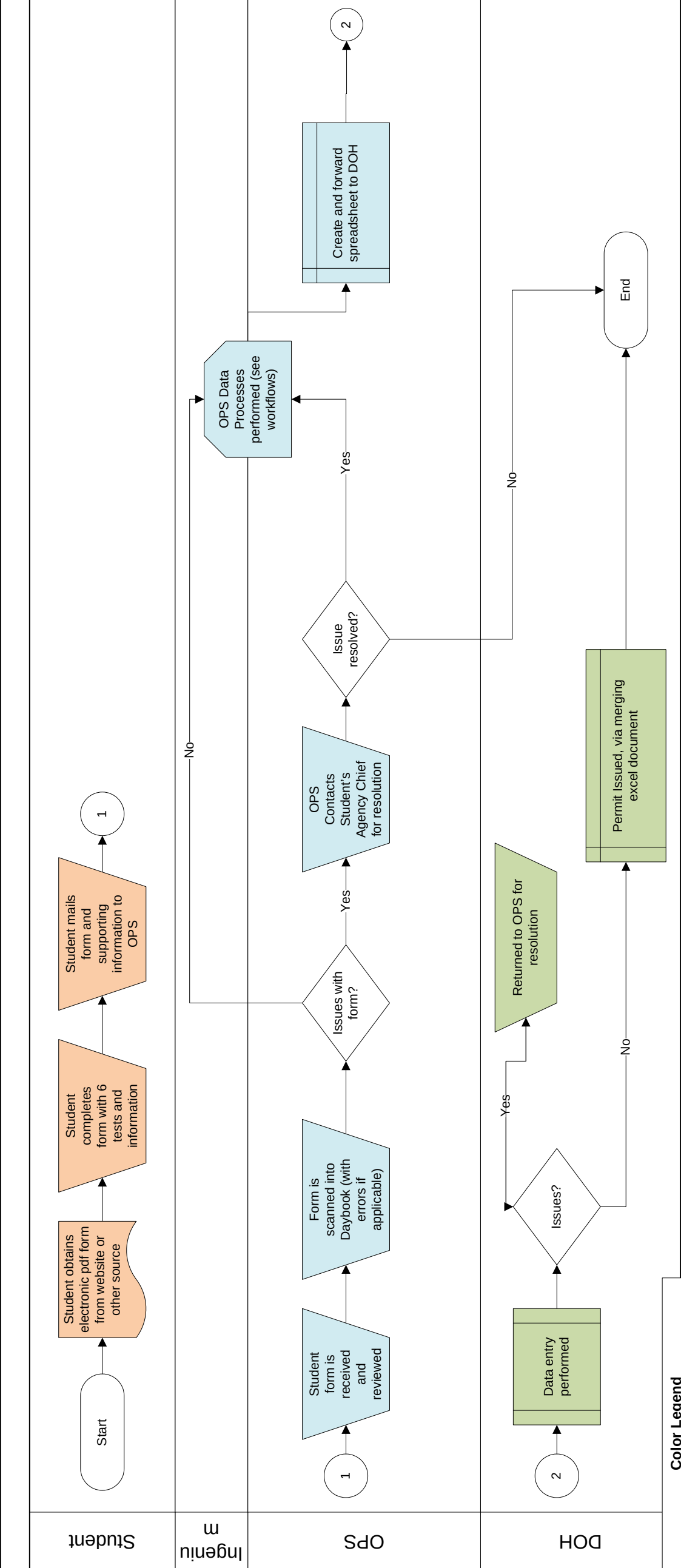


6 Test Breath Analysis Operator – Current Process



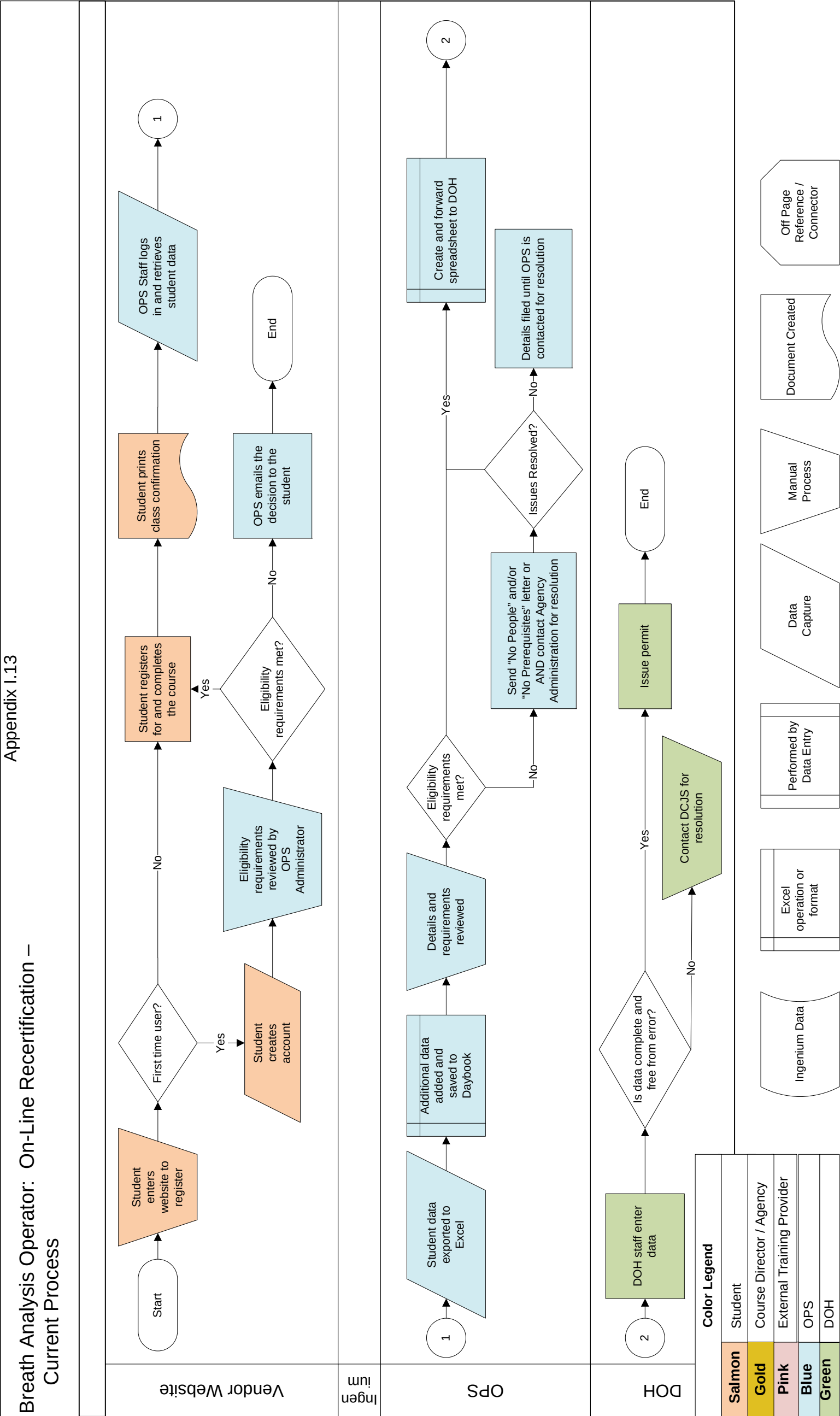
Color Legend					
Gold	Course Director / Agency				
Salmon	Student				
Pink	External Training Provider				
Blue	OPS				
Green	DOH				
		Excel operation or format	Performed by Data Entry	Data Capture	Manual Process
		Ingenium Data	Document Created	Off Page Reference / Connector	

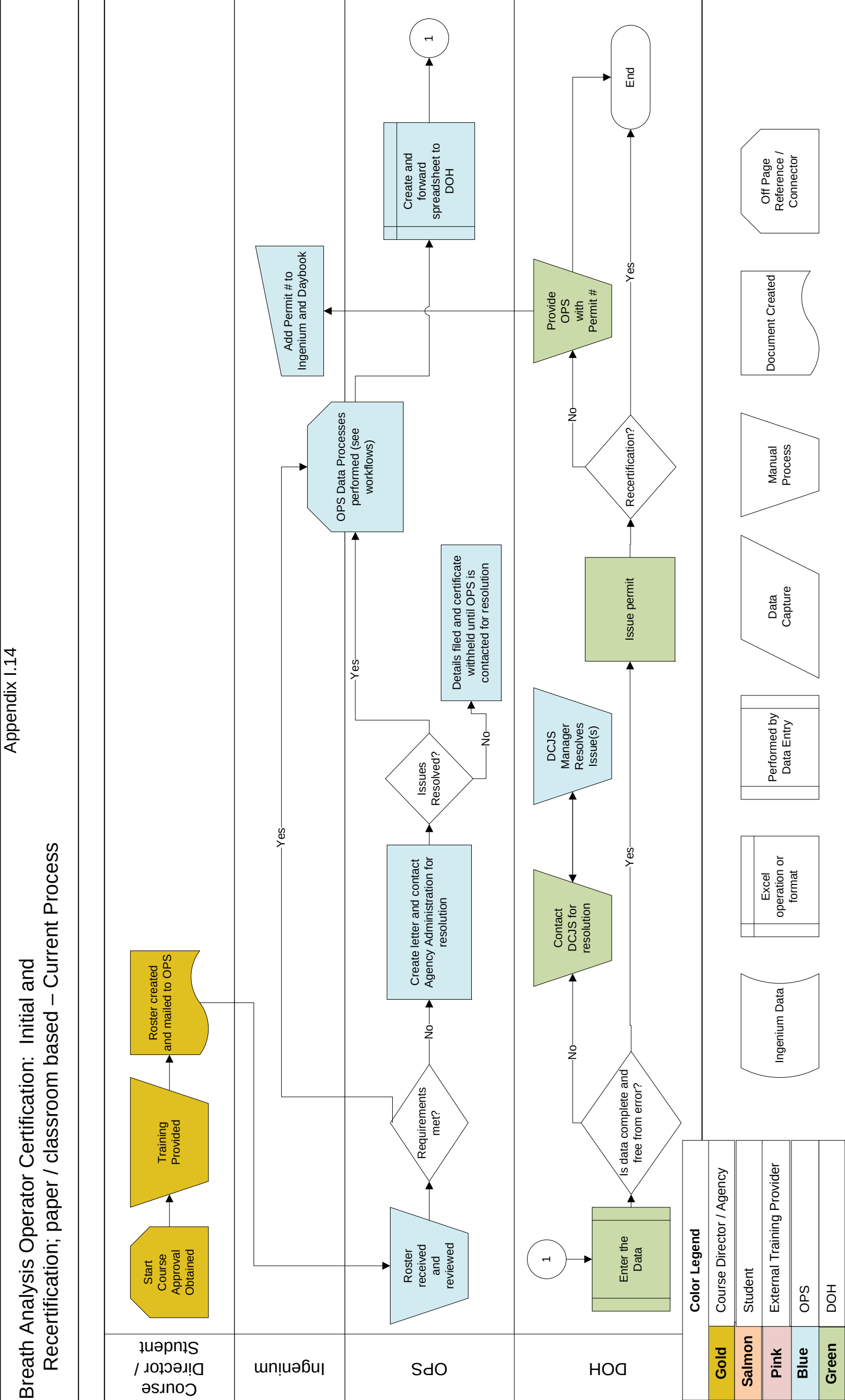
6 Test Breath Analysis Operator Recertification
(paper based) – Current Process

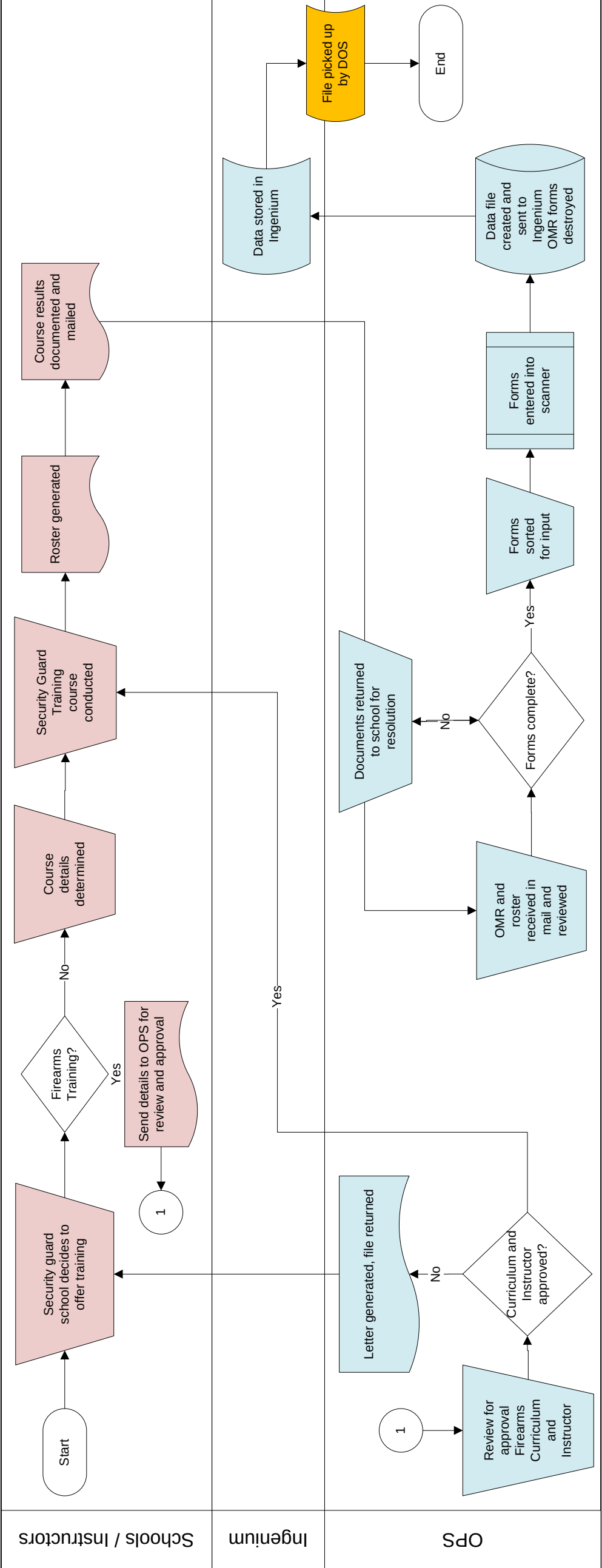


Gold	Course Director / Agency
Salmon	Student
Pink	External Training Provider
Blue	OPS
Green	DOH

Ingenium Data	Excel operation or format	Performed by Data Entry	Data Capture	Manual Process	Document Created	Off Page Reference / Connector

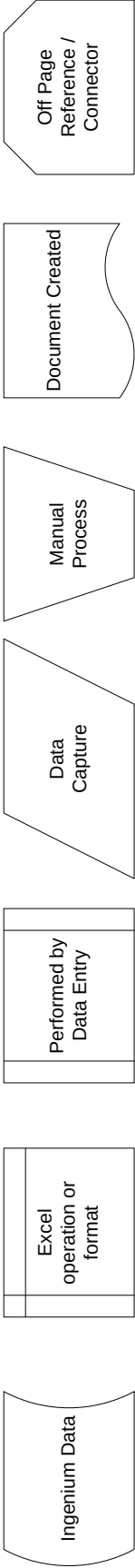






Color Legend	
Gold	Course Director / Agency
Salmon	Student
Pink	External Training Provider
Blue	OPS
Green	DOH

- Assumes that schools and Instructors are approved to teach unarmed Security Guard Training
- Schools are responsible for confirming that each student can take the class



Appendix J

Change Request Form

Intentionally Blank

**Appendix J
Change Request Form
CJS 2014 01**

Description of Requested Change:
Reason/Justification for Change:
Additional or Deleted Tasks or Deliverables Required by Change:
Additional or Deleted Cost and/or Timeframes Required by Change:

The signatures below represent that New York State and (insert Offerer/vendor company name) are in agreement with the above change(s) to the project deliverables for the CJS 2014 01 Service Agreement.

New York State	(insert Offerer/vendor company name)
Name (Print):	Name (Print):
Signature:	Signature:
Title:	Title:
Date:	Date:

This Page Intentionally Blank

Appendix K

OPS Business Requirements

Intentionally Blank

Appendix K

Table 1a - Report Requirements

The table below lists the standard reports currently produced by DCJS staff to meet business requirements and customer needs. The proposed system must allow DCJS to produce these standard reports as well as create *ad hoc* reports from any of the reports.

Item #	Standard Report Name	Frequency	Who Receives	Delivered How?	Purpose (what does the report tell the reader)
1	Training Completed By Agency	Daily	Agencies, public	Adobe/Excel	The names of employees and their training
2	Training Completed By Topic	Daily	Agencies, Academies, Public	Adobe	All Students who have completed a training course
3	Instructors	As needed	Agencies, Academies, Public	Adobe	Qualifications by topic and location (county and training zone)
4	Individual Training Record	Daily	Agencies, Individuals, Public	Adobe/Excel	Transcript of employment and training
5	Individual Training Record (SGP)	Daily	Agencies, Individuals, Public	Adobe/Excel	Transcript of Security Guard Program (SGP) training
6	Contact Report	Monthly	Deputy Commissioner/Public	Excel	Contact information for police/peace agencies
7	GTSC Grant Report	Annually	OPS Staff/Public	Adobe/Excel	Training statistics for traffic safety programs
8	Total number of police officers	Daily	OPS Staff/Public	Adobe/Excel	Current total of police officers (active on Registry)
9	Total number of peace officers	Daily	OPS Staff/Public	Adobe/Excel	Current total of peace officers (active on Registry)
10	Total number of police employers	Daily	OPS Staff/Public	Adobe/Excel	Current total of police officer employers
11	Total number of peace employers	Daily	OPS Staff/Public	Adobe/Excel	Current total of peace officer employers
12	Police officers by CPL designation	Daily	OPS Staff/Public	Adobe/Excel	Total # of Police Officers in each CPL designation
13	Peace officers by CPL designation	Daily	OPS Staff/Public	Adobe/Excel	Total # of Peace Officers in each CPL designation
14	Police Agencies by Size	Daily	OPS Staff/Public	Adobe/Excel	Total # of Police Officers Employed
15	Peace Agencies by Size	Daily	OPS Staff/Public	Adobe/Excel	Total # of Peace Officers Employed
16	Latent Print Examiners	Quarterly	DCJS Staff/Public	Adobe	Certification status of latent Print Examiners
17	SGP Approved Schools	Monthly	DCJS Staff/Public	Adobe	Approved Security Guard Schools
18	SGP Approved Instructors	Monthly	DCJS Staff/Public	Adobe	Approved Security Guard Instructors
19	SGP Events Taught	Daily	DCJS Staff/Public	Adobe	Security Guard Courses Completed
20	SGP Suspended/Revoked	Daily	DCJS Staff/Public	Adobe	Security Guard School Suspension and Revocations
21	Registry Validation Report	Annually	DCJS Staff/Agencies/Public	Adobe	Details based on agency ID/Job Title
22	Routine Correspondence	Daily	Agencies/Academies/Public	Adobe	Based on actions taken within LMS (notifications)
23	Employees by Agency (current and former)	Daily	OPS Staff	Adobe/Excel	Lists entire registry for a given agency or category
24	Active/Inactive Courses (by code or name)	Daily	OPS Staff	Adobe/Excel	Lists all active or inactive course titles
25	Registry Tracking Report	Daily	OPS Staff	Adobe/Excel	Monitor/count all registry activity (total, by classification, and by agency)
26	Accredited Agencies	Daily	OPS Staff	Adobe/Excel	Monitor/count Accredited agencies (total, by classification, and by agency)

Appendix K

Table 1b - Statistical Report Requirements

The table below lists the statistical reports produced to document work output of DCJS staff. The data for each report is displayed in a month to month and year to year history for the current calendar year. The proposed system must allow DCJS to produce these standard statistical reports as well as create adhoc statistical reports.

Item #	Statistics Report Name	Frequency	Who Receives	Delivered How?	Purpose (what does the report tell the reader)
1	OPS Monthly Report (Performance statistics)	Monthly, Annually	DCJS Staff/Deputy Commissioner	Adobe/Excel	Monthly Summary of overall Staff performance, volume, numbers trained, etc.. (See items 2-14 below)
2	Number of training courses approved	Monthly, Annually	DCJS Staff/Deputy Commissioner	Adobe/Excel	Volume of current work flow compared to a 3 year history
3	Training courses completed	Monthly, Annually	DCJS Staff/Deputy Commissioner	Adobe/Excel	Total # of courses delivered
4	Individual records updated	Monthly, Annually	DCJS Staff/Deputy Commissioner	Adobe/Excel	The # of record updates made by DCJS Staff
5	Persons trained	Monthly, Annually	DCJS Staff/Deputy Commissioner	Adobe/Excel	Total # of persons completing training courses
6	Training Completion Certificates issued	Monthly, Annually	DCJS Staff/Deputy Commissioner	Adobe/Excel	Total # of Training Certificates issued
7	Pistol Permit Verifications Completed (by New York State Police)	Monthly, Annually	DCJS Staff/Deputy Commissioner	Adobe/Excel	Total # of records verified by State Police Staff
8	Freedom of Information Law (FOIL) requests completed	Monthly, Annually	DCJS Staff/Deputy Commissioner	Adobe/Excel	Total # of records provided
9	Adhoc executive requests for reports	Monthly, Annually	DCJS Staff/Deputy Commissioner	Adobe/Excel	Total # of special requests completed by staff
10	Employer requests for records updates	Monthly, Annually	DCJS Staff/Deputy Commissioner	Adobe/Excel	Total # of records provided
11	Individual requests for updates or transcripts, and instructors certified	Monthly, Annually	DCJS Staff/Deputy Commissioner	Adobe/Excel	Total # of records provided
12	Registry transactions Per Month	Monthly, Annually	DCJS Staff/Deputy Commissioner	Adobe/Excel	Total # of Police and Peace Officers added and removed from the registry per month
13	Registry transactions Year to Date	Monthly, Annually	DCJS Staff/Deputy Commissioner	Adobe/Excel	Total # of Police and Peace Officers added and removed from the registry per year
14	Registry transactions Three Years to Date	Monthly, Annually	DCJS Staff/Deputy Commissioner	Adobe/Excel	Total # of Police and Peace Officers added and removed from the registry in last three years

Appendix K

Table 2 - User Population

The table below depicts the current Training Courses recognized by DCJS and labeled in the Ingenium interface as "Learning Experiences."

Item #	Agency, Role, Source	Role within the Agency, if applicable	*Approx # of users	Process / Requirement	Comments
1	Police Officer Employers*	HR Administrator	588	Maintain registry	
2	Peace Officer Employers*	HR Administrator	1816	Maintain registry	
3	Police Officers	User	66936	Enroll in training	Number is total population of police officers
4	Peace Officers	User	99636	Enroll in training	Number is total population of peace officers
5	Training Academies/Civilian Partners*	Support Administrator	60	Administer training courses	Civilian partners= mental health orgs, civil service, etc.
6	Civilians (law enforcement)	User	1000	Enroll in training, deliver training	Certain instructors are non-sworn persons
7	Security Guards (Civilians)	User	225000	Enroll in training	If limited to schools only, number is 600
8	Security Guard Schools*	Support Administrator	500	Administer training courses	
9	Security Guard Instructors	Support Administrator	2300	Administer training courses	
10	OPS Staff	Primary Administrator	3	Administer LMS for OPS	
11	OPS Staff	Secondary Administrator	45	Administer training courses/records	Law Enforcement Training Unit/Admin Unit: approve, reject, certify students and curricula
12	Department of Health	Secondary Administrator	1	Learner transcripts	Receive training data from DCJS OPS for BAO Program
13	Department of State	Secondary Administrator	1	Learner transcripts	Receive training data from DCJS OPS for SGP
14	Department of Homeland Security and Emergency Services	HR Administrator	1	Retrieve police and peace registry data	For use with pending Statewide ID program
15	MY Smart Simulations, Inc.	Secondary Administrator	1	Receive personnel data and transmit completion rosters	
16	New York State Police	Secondary Administrator	1	Pistol License Verification	NYSP to be able to access PPRST to verify peace officer category of individuals attempting to purchase firearms with credentials. Mandate: required by Executive Law 845.
Total User Population			395,485		
*Total Employer Population			2,964		

Appendix K

Table 3 - Business Processes

The table below depicts the current Business Processes.

Item #	Name	Frequency	Inputs	Outputs	Comments
1	Maintenance of the Registry	Daily	Police/peace employers	Police/peace employers/OPS/FOIL	Mandate: required by Exec 845. Seeking self-service model.
2	Annual Validation of the Registry	Annually	OPS	Police/peace employers/OPS/FOIL	Mandate: required by Exec 845. Seeking self-service model. All agency CEOs must verify annually on January 15th all information and persons employed by their agency.
3	Course Approval (Police and Peace)	Daily	Police/peace employers/academies	Police/peace employers/OPS/FOIL	Mandate: required by Exec 841.
4	Issuance of certifications/approvals	Daily	Agencies/Academies/SGP Schools	Agencies/Academies/Public	Mandate: required by Exec 841. Pushed out automatically.
5	Certification Maturity Date	Daily	OPS Staff	Police/peace employers/OPS/FOIL	Policy: Certain certification have maturity dates of varying length...fingerprints, BAO, SWAT, etc.
6	Basic Training Gap Analysis	Daily	OPS Staff	Police/peace employers/OPS/FOIL	Mandate: General Municipal Law 209-q and Criminal Procedure Law 2.30. Durational validity of certificate and the amount of time one may be separated from police or peace officer service before the certificate expires.
7	Pistol License Verification	Daily	NYSP	NYSP	Mandate: required by Exec 845.
8	Security Guard Training Records	Daily	SGP Schools	Dept. of State/Student/OPS	Mandate: required by Exec 841-c. Seeking self-service model.
9	Security Guard School Approval	Daily	SGP School Applicants	Public	Mandate: required by Exec 841-c.
10	Security Guard Instructor Approval	Daily	SGP Instructor Applicants	Public	Mandate: required by Exec 841-c.
11	Identify For-profit/Non-for-Profit Security Guard Schools	Daily	OPS Staff	OPS Staff	Identify which schools are non-profit to avoid charging fees for school and instructor certification.
12	Security Guard School Maturity Date	Daily	OPS Staff	Public	Mandate: required by 9 NYCRR 6027. School certifications should have and effective date and 2 yr. maturity date.
13	Security Guard Instructor Maturity Date	Daily	OPS Staff	Public	Mandate: required by 9 NYCRR 6029. School certifications should have and effective date and 5 yr. maturity date.
14	Training Announcements	Daily	OPS Staff	Police/peace officers and employers/Public	Push notifications to learners/learner groups.
15	Ad-hoc Reporting (training records/stats.)	Daily	OPS Staff/Agencies/Academies/Individuals	OPS Staff/Agencies/Academies/Individuals	See Reporting Tab.
16	Data Entry of Rosters	Daily	Agencies/Academies/SGP Schools	Agencies/Academies/SGP Schools/Public	Mandate: required by Exec 841, 841-c. Seeking self service model and bulk upload.
17	Track correspondence and record	Daily	OPS Staff/Agencies/Academies/Individuals	OPS Staff/Agencies/Academies/Individuals	Track notifications and letters sent via SLMS
18	Provide On-line Learning	Daily	OPS staff	Agencies/Academies/SGP Schools/Public	Deliver on-line training content to registered users

Appendix K

Table 3 - Business Processes

Item #	Name	Frequency	Inputs	Outputs	Comments
19	Manage pre-established pre-requisites to register for training/certification	Daily	User base	User base, CEOS, Public	Mandate: required by Exec 841 and agency policy. Automatically identify pre-requisites and allow/deny registration based on pre-requisites.
20	Identify County of Organizations	Daily	OPS Staff	OPS Staff	Capture county or origin for sorting/reporting purposes
21	Identify Training Zone	Daily	OPS Staff	OPS Staff	Capture OPS training zones (14) for sorting/reporting purposes
22	Customize notifications for course approval and certification processes	Daily	OPS Staff	OPS Staff/Agencies/Academies/Individuals	Routine correspondence based on actions taken in SLMS [approval, certification, denial, not registered (police or peace), etc.]
23	Create fluid notifications or letters for unique situations	Daily	OPS Staff	OPS Staff/Agencies/Academies/Individuals	Semi-routine correspondence based on unique or combination circumstances - not registered (police or peace) and no prerequisite or rejected registry forms, etc...
24	Law Enforcement Accreditation Program	Daily	OPS Staff	OPS Staff/Agencies/Academies/Public	Identify agencies that are accredited (voluntary program for professionalization)
25	Create Notifications for Law Enforcement Accreditation Program	Daily	OPS Staff	OPS Staff/Agencies/Academies/Public	Accreditation dates, assessment notices, reaccreditation dates, etc.
26	Publish and maintain Law Enforcement Accreditation Program Standards	Daily	OPS Staff	OPS Staff/Agencies/Academies/Public	

Table 4 - User Access Levels (Desired)

User Functions

Access Level	User Titles		Access															Estimated Users
	(Individual user descriptions on page 2)		Update Personal contact info	View & Print Personal Record	Enroll in Training (In-residence or On-line)	Perform Employee Validation	Edit/Update Employee Records	Print Agency Training Reports	Submit Curriculum Forms for DCJS Approval	Submit Class Rosters	Extract Specific Program Data to a Report	Add/create On-line Training Content	Add/Create new Category of Peace & Police Officers	Add/Create Training Courses	Delete Records	Assign/Modify User Access Levels		
1	Record Holders (Police & Peace Officers)		✓	✓	✓	✓	✓	✓	✓	✓							100,000	
2	Training Managers (Police & Peace Officers)		✓	✓	✓	✓	✓	✓	✓								4,000	
3	DCJS Administrative Staff		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		40	
4	DCJS Senior Administrative Staff		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	3	
5	Training Managers (Security Guard Program)		✓	✓	✓	✓	✓	✓	✓								500	
6	Record Holders (Security Guards)		✓	✓													200,000	
7	NYS Department of Health Staff									✓							2	
8	NYS Dept. of State Staff									✓							2	
9	NYS DHSES									✓							2	
10	NYS State Police Staff									✓							2	
11	IMY Smart Simulations, Inc. Staff									✓							2	

Appendix K

Table 4a - User Definitions

The table below provides individual user descriptions of duties and corresponding required system access.

Level	User Descriptions
1	Record Holders (Police & Peace Officers): Individuals listed on the Police and Peace Officer Registry. Able securely access their own personnel record. Enroll in training courses either in residence or on-line. Limited to viewing and printing their own personnel record and updating personal contact information such as an email address and/or phone number.
2	Training Managers (Police & Peace Officers): Persons designated and authorized to perform administrative functions and records maintenance for all members assigned to their organization on behalf of a user agency or employer of persons on the Police and Peace Officer Registry. These persons include Chief, Sheriff, and/or designated training managers for every department listed in the Management Database. These individuals will also be capable of submitting for DCJS approval training related materials, not limited to, but including, course approval forms and class rosters.
3	DCJS Administrative Staff: performing records updates; generating reports; statistics and audits, managing training course enrollment and adding content for on-line training.
4	DCJS Senior Administrative Staff: Full Authority including capability to grant/determine/approve access level to all system users.
5	Training Managers (Security Guard Program): Persons authorized to perform administrative functions and records maintenance for all members assigned to their organization on behalf of a user agency or employer of persons on the Security Guard Registry. These individuals will also be capable of submitting for DCJS approval training related materials, not limited to, but including, course approval forms and class rosters. Cannot delete records. Cannot access records maintained in the Peace and Police Officer registry.
6	Record Holders (Security Guards): Individual employees who are individual record holders listed on the Security Guard Registry. Limited to viewing and printing their own personnel record and updating personal contact information such as an email address and/or phone number.
7	NYS Department of Health Staff: State entity requiring access to retrieve training data from DCJS Peace & Police Registry for Breath Analysis Operator Program.
8	NYS Department of State Staff: State entity requiring access to retrieve data from DCJS for Security Guard Program
9	NYS Department of Homeland Security and Emergency Services (DHSES): State entity requiring access to retrieve data from DCJS Peace & Police Registry for use with pending Statewide Credentialing program for first responders
10	NYS State Police Staff: State entity performing Pistol License Verification. Requiring access to view Registry records of Police & Peace Officers to verify retrieve to verify peace officer category of individuals attempting to purchase firearms with credentials.
11	MY Smart Simulations, Inc. Staff: Private vendor requiring access to retrieve data and transmit completion rosters.

Appendix K

Table 5 - Learning Experiences

Course Code	Course Name	Pre-Requisites Courses	Appointment type	Certificate Type	Notes
1	Basic Course for Police Officers		Appointed Police Officer	MPTC	
4	Course in Police Supervision	001 or 502 Police Basic Training	Appointed Police Officer	MPTC	
5	Executive Development Seminar			DCJS	
21	Miscellaneous In-Service Course			DCJS	This code is to file courses that do not have an established DCJS course code or an MPTC training standard established.
36	Hostage Negotiation Course			MPTC	
37	Crisis Intervention Instructor Course		Affiliated with Peace or Police Agency or	DCJS	
39	Basic Crash Management Course			DCJS	See course codes 158, 159.
40	Intermediate Crash Management Course	39 Basic Crash Management		DCJS	See course codes 158, 159. □
41	Advanced Crash Management	40 Intermediate Crash Management		DCJS	See course codes 158,159. □
42	Technical Crash Management	41 Advanced Crash Management		DCJS	See course codes 158,159. □
46	Advanced Police Photography Course			DCJS	
47	Radar Operator Course			MPTC	
61	Mounted Police Officer Course			MPTC	
69	Advanced Police Juvenile Officers Course			DCJS	
109	Fundamentals of Community and Problem Oriented Policing			DCJS	
113	Law Enforcement Bicycle Patrol Course		Appointed Police or Peace	MPTC	
114	Police Officer Refresher Course		Appointed Police Officer	MPTC	
115	Specialized Investigator Police Training Course		Appointed Police	MPTC	
117	Standard Marine Patrol Vessel Operator Course			DCJS	
121	Marine Law Enforcement Course			DCJS	

Appendix K

Table 5 - Learning Experiences (Continued)

Course Code	Course Name	Pre-Requisites Courses	Appointment type	Certificate Type	Notes
124	Critical Incident Management Facilitator Course			MPTC	
126	Drug Interdiction Instructor Course			MPTC	
127	Interview and Interrogation Course			DCJS	
129	Basic Course for Peace Officers with Firearms (Police Basic) 1-1-87		Former Police now Peace	None	This code is for peace officers who attended a basic course for police officers after the MPTC ruled that peace officers would no longer be eligible for a police certificate.
130	Highway Drug Interdiction Course			MPTC	
132	Police Crime Scene and Evidence Specialist Course	440 Basic Investigative Photography		MPTC	
135	Basic Course for Police Officers Equivalency - NYSP/NYPD		Former NYPD or NYSP	None	This is to provide equivalency certification for police officers appointed by a municipality who successfully completed police officer basic training while members of the New York State Police or police officers who completed police basic training at the New York City Police Department
136	Mental Health Instructor Course	250 General Topics Instructor		MPTC	
141	General In-Service Course for Police Officers			MPTC	MPTC approved updated curriculum and title to reflect approved course name and target audience based on Police on Police Shooting Task Force recommendations. Duration 21 hours.
143	Domestic Violence Instructor Course	250 General Topics Instructor		MPTC	
144	Impaired Boaters Recognition Course			DCJS	
146	Accreditation Assessor Seminar			DCJS	This seminar is to train persons to complete the assessment of a law enforcement agency seeking accreditation from the NYSLEAP pursuant to 9NYCRR 6035..
148	Firearms Transitional Course			DCJS	This code is for programs that transition officers from revolvers to semi-automatic pistols.
149	Domestic Violence Course			DCJS	
151	Drug Recognition Expert Course 2 Day			MPTC	

Appendix K

Table 5 - Learning Experiences (Continued)

Course Code	Course Name	Pre-Requisites Courses	Appointment type	Certificate Type	Notes
152	Drug Recognition Expert Course 7 Day			MPTC	
153	Drug Recognition Expert Recertification Course			MPTC	
155	Drugs That Impair Driving Course	183 DWI & SFST		MPTC	
161	Basic Criminal Investigations Course			MPTC	
162	Basic Juvenile Officers Course			MPTC	
174	Victim Witness Assistance Program			DCJS	
183	DWI Detection and SFST Course	001 or 502 Police Basic Training		MPTC	
184	Commercial Vehicle Enforcement Seminar			DCJS	
185	Latent Print Processing Course - Level I			MPTC	
186	Advanced Latent Print Training - Level II	185 Latent Print Processing Course - Level I		MPTC	
187	Certified SABIS Latent Print Examiner Course - Level III	186 Advanced Latent Print Training - Level II		MPTC	
188	Extension: Basic Course for Police Officers			None	
189	Extension: Course in Police Supervision			None	This code is used to identify police officers who have been granted an extension of the time frame for completion of the Basic Course for Police Officers due to exigent circumstances pursuant to 9 NYCRR 6021.7(b). The time frame cannot exceed two years from the original date of appointment as a first-line supervisor.
191	Extension: Basic Course for Peace Officers			None	This code is used to identify peace officers or campus public safety officers who have been granted an extension of the time frame for completion of the Basic Course for Peace Officers or other MPTC approved basic training program, such as the Campus Public Safety Officer Course, due to exigent circumstances pursuant to 9 NYCRR 6025.7(b). The time frame cannot exceed two years from the original date of appointment as a peace officer.

Appendix K

Table 5 - Learning Experiences (Continued)

Course Code	Course Name	Pre-Requisites Courses	Appointment type	Certificate Type	Notes
200	Police Patrol Canine Course	001 or 502 Police Basic Training		MPTC	
201	Police Patrol Canine Certification	001 or 502 Police Basic Training		MPTC	
203	Police Tracking Canine Course	001 or 502 Police Basic Training		MPTC	
204	Police Tracking Canine Certification	001 or 502 Police Basic Training		MPTC	
206	Police Article Search / Scent Detection Canine Course	001 or 502 Police Basic Training		MPTC	
207	Police Article Search / Scent Detection Canine Certification	001 or 502 Police Basic Training		MPTC	
209	Police Canine In-Service Training Program	001 or 502 Police Basic Training		DCJS	
213	Police Field Training Officer Course	001 or 502 Police Basic Training		MPTC	This 28 hour course has been developed to familiarize police officers with the basic elements of, and methods used in the National Field Training and Evaluation Program. □ 9/18/2013 MPTC approved proposal to require all FTOs for the 160 (required) hours of SFTR&O have attended an MPTC approved FTO course. This requirement will go into effect for BCPOs commencing after 1/1/2015.
214	Street Encounters Course			MPTC	
215	Advanced Street Encounters Course			MPTC	
226	Suicide TTT Phase I			None	
227	Suicide TTT Refresher			None	
228	Staff Sexual Misconduct TTT			None	
229	Sexual Harassment Prevention TTT			None	

Appendix K

Table 5 - Learning Experiences (Continued)

Course Code	Course Name	Pre-Requisites Courses	Appointment type	Certificate Type	Notes
230	Basic Investigative Photography Course - Equivalency			MPTC	This code is used to denote officers who have completed a law enforcement photography course and who have successfully completed the written and practical examinations portions of the MPTC Basic Investigative Photography Course for the purpose of meeting the pre-requisite requirement for the MPTC Crime Scene and Evidence Specialist Course. Such equivalent courses include: the FBI Basic Photography course.
231	Personal Awareness TTT			DCJS	
232	New Correctional Supervision TTT			DCJS	
233	Legal Issues TTT			DCJS	
234	Juvenile Custody TTT			DCJS	
235	Intro Direct Supervision TTT			DCJS	
236	Interpersonal Communications TTT			DCJS	
237	SCOC 40 Hour Instructor Development			None	
238	Inmate Classification TTT			DCJS	
239	Inmate Class/Trainers & Class Officers			DCJS	
240	Fire Protection TTT			None	
241	Effective Communication TTT			None	
242	ECHO TTT			None	
243	Direct Supervision Line Staff TTT			DCJS	
244	SCOC Chemical Agents 40 Hour TTT			None	
245	SCOC Chem Agents (Aerosols) TTT			None	
246	Drug Recognition Expert Instructor Course	250 IDC		MPTC	These instructors are approved to teach the DWI Detection and SFST Course, Drugs that Impair Driving Course, and Drug Recognition Expert Courses. ☐
247	Campus Public Safety Officers Course		Appointed by a Campus	MPTC	
248	Campus Public Safety Officer Course - Equivalency/Waiver	248	Prior Police Basic Training	MPTC	
249	Master Instructor	250 General Topics Instructor		DCJS	
250	Instructor Development Course - General Topics			MPTC	

Appendix K

Table 5 - Learning Experiences (Continued)

Course Code	Course Name	Pre-Requisites Courses	Appointment type	Certificate Type	Notes
252	Firearms Instructor Course	250 IDC	3 Year Police Peace w/ a FA	MPTC	
254	Defensive Tactics Instructor Course			DCJS	
255	Defensive Tactics Instructor Recertification			DCJS	
256	Chemical Agents Instructor Course		Appointed Police or Peace	DCJS	
257	Chemical Agents Instructor Recertification	256 Chemical Agents Instructor		DCJS	
258	Ethical Awareness Moderator Course			MPTC	
259	Ethical Awareness Moderator Recertification			DCJS	
260	Radar Instructor Course	47 Radar Operator Course		MPTC	This course is designed to assist officers in the instruction of the Radar Operator Course (code 47).
262	Instructor Evaluator Workshop			MPTC	
263	DARE Officer Training Course			MPTC	
264	DARE Officer Recertification	263 DARE Officer Training Course		MPTC	
265	Highway Drug Interdiction Instructor Course	130 Highway Drug Interdiction Course		MPTC	
266	Highway Drug Interdiction Instructor Recertification	265 Highway Drug Interdiction Instructor Course		MPTC	
267	DARE/Mentor			MPTC	
268	DARE Met of TR Recert			MPTC	
272	EVOC Instructor Course			MPTC	
273	EVOC Instructor Recertification			MPTC	
274	Drug Field Test Instructor Course			MPTC	
278	DARE Junior High Course			MPTC	
279	DARE High School Course			MPTC	
280	DARE Parent Course			MPTC	
285	DARE Elementary Curriculum Update			MPTC	
286	DARE Middle School Curriculum Update			MPTC	
287	DARE Junior High Recertification			MPTC	
288	DARE Senior High Recertification			MPTC	
289	DARE Parent Recertification			MPTC	

Appendix K

Table 5 - Learning Experiences (Continued)

Course Code	Course Name	Pre-Requisites Courses	Appointment type	Certificate Type	Notes
290	DARE Elementary Update Course 1998			MPTC	
292	DARE Elementary Curriculum Update 2003 Phase II			MPTC	
293	DARE Elementary Curriculum Update 2003 Phase I			MPTC	
294	Physical Fitness Instructor Course			MPTC	
295	Occupant Protection Use Enforcement Instructor Course			DCJS	
301	Stress Management Instructor Course			DCJS	
302	Narcotics Detection Canine Course	001 or 502 Police Basic Training		MPTC	
303	Narcotics Detection Canine Team Certification	001 or 502 Police Basic Training		MPTC	
304	Explosive Detection Canine Course	001 or 502 Police Basic Training		MPTC	
305	Explosive Detection Canine Team Certification	001 or 502 Police Basic Training		MPTC	
306	Police Canine Trainer Course	001 or 502 Police Basic Training		MPTC	
307	Police Canine Trainer Certification	001 or 502 Police Basic Training		MPTC	5 year expiration date.
308	Police Canine Maintenance Trainer Certification	001 or 502 Police Basic Training		MPTC	5 year expiration date.
309	Police Canine Examiner Course	001 or 502 Police Basic Training		MPTC	
310	Police Canine Examiner Certification	001 or 502 Police Basic Training		MPTC	5 year expiration date.
311	Firearms Instructor-In Service			DCJS	
312	Canine Handlers Explosives Awareness Course	001 or 502 Police Basic Training		MPTC	
313	DARE Junior High Update Course 2003			MPTC	
314	Drug Recognition Expert Recertification			MPTC	
315	DARE Supplemental Lessons			MPTC	
316	DARE Phase III On-Line Elementary			MPTC	
317	DARE Phase III On-Line Middle School			MPTC	

Appendix K

Table 5 - Learning Experiences (Continued)

Course Code	Course Name	Pre-Requisites Courses	Appointment type	Certificate Type	Notes
320	Certified SABIS Latent Print Examiner	321 Certified Latent Print Examiner		MPTC	Certificate has a 3 year expiration date pursuant to MPTC approved course.
321	Certified Latent Print Examiner			MPTC	☐ Certificate will have a 1 year expiration date. OFOPS to forward annual rosters accordingly. ☐
322	Certified SABIS Latent Print Examiner Recertification	320 Certified SABIS Latent Print Examiner		MPTC	MPTC-Cert 3 year expiration.
323	Certified Latent Print Examiner Re-Certification	321 Certified Latent Print Examiner		MPTC	2/20/2007 - Certificate has a 1 year expiration date.
324	Certified Latent Print Examiner - Annual Proficiency Test	321 Certified Latent Print Examiner		MPTC	
350	Aerosol Subject Restraint Instructor Course	362 Aerosol Subject Restraint Course		MPTC	
357	Commercial Vehicle Weight & Permits Seminar			DCJS	
359	Respond Missing/Abducted Children (REMAC) Seminar			DCJS	
361	Public Information Officer Course			MPTC	
362	Aerosol Subject Restraint Course		Appointed Police or Peace	MPTC	
363	Instructor Development Conversion Course			MPTC	The purpose of this program is to upgrade the training of students who have completed instructor courses that do not meet the standards established by the MPTC for the Instructor Development Course prior to 1996
375	Lidar Operator Upgrade Course	47 Radar Operator Course		MPTC	
376	Radar/Lidar Operator Course		Appointed Police or Peace	MPTC	
377	Lidar Instructor Upgrade Course	260 Radar Instructor Course		MPTC	

Appendix K

Table 5 - Learning Experiences (Continued)

Course Code	Course Name	Pre-Requisites Courses	Appointment type	Certificate Type	Notes
393	Breath Analysis 6-Test Renewal	Breath Analysis Course		None	Renewal on the DataMaster and/or Alcotest for officers who had been previously certified on these instruments by the basic, upgrade or recertification course. Cannot be done two consecutive times.
400	Non Certified Special Topic Instructor			None	Qualified to instruct a special topic without MPTC certification.
402	Breath Analysis Operator Course			MPTC	
403	Breath Analysis Upgrade Course	402 Breath Analysis Operator Course		DCJS	
404	Breath Analysis Recertification	402 Breath Analysis Operator Course		MPTC	
405	Breath Analysis Instructor Update/Recertification Course	406 Breath Analysis Instructor Course		DCJS	
406	Breath Analysis Instructor Course			MPTC	
409	Suicide Prevention & Crisis Intervention Instructor Course			DCJS	
411	Crime Analyst Certification - Level 1			MPTC	
418	Police Sniper Course - Level I		Appointed Police Officer	MPTC	
419	School Resource Officer Course			DCJS	
420	Counter Terrorism Instructor Course	422 Counter Terrorism Awareness		MPTC	
421	Advanced School Resource Officer Course	419 School Resource Officers		DCJS	
422	Counter Terrorism Awareness Course - Introductory			MPTC	
423	Counter Terrorism Awareness Course - Intermediate			MPTC	
424	Weapons of Mass Destruction Course			MPTC	
425	Counter Terrorism Executive Seminar			DCJS	
426	Law Enforcement Response to Weapons of Mass Destruction Instructor Course			None	
427	Incident Response to Terrorist Bombings Course			None	
428	Stress Management Seminar			None	

Appendix K

Table 5 - Learning Experiences (Continued)

Course Code	Course Name	Pre-Requisites Courses	Appointment type	Certificate Type	Notes
429	School Resource Officer Supervisor Course			DCJS	
430	Fraudulent Documents Course			None	
431	Youth Gangs, Guns and Drugs Seminar			DCJS	
432	Counter Terrorism Awareness for Peace Officers			DCJS	
433	Basic Crime Prevention Officer Course			MPTC	
436	Radar/Lidar Instructor Course	376 Radar/Lidar Operator Course		MPTC	
437	DWI Detection and SFST Instructor Course	183 DWI Detection & SFST Course		MPTC	
438	DWI Detection and SFST Instructor Course Recertification	437 DWI Detection and SFST Instructor Course		DCJS	
439	NYS Law Enforcement Executive Institute			DCJS	
440	Basic Investigative Photography Course			MPTC	
441	Property/Evidence Room Management			DCJS	
442	Conducted Energy Device Course		Appointed Police or Peace	MPTC	
443	SWAT Operator Course	001 or 502 Police Basic Training		MPTC	
444	SWAT Operator Equivalency	001 or 502 Police Basic Training		MPTC	
445	SWAT In-Service Course	SWAT Operator/Equivalency		MPTC	
446	Conducted Energy Device - Equivalency		Appointed Police or Peace	MPTC	
447	SWAT Team Certification	SWAT Team		MPTC	This signifies a SWAT team has met the minimum standards for certification.
448	Patrol Rifle Course	Police Basic Training or Peace Basic with Firearms			
500	Consultant Instructor 2004-2009			None	

Appendix K

Table 5 - Learning Experiences (Continued)

Course Code	Course Name	Pre-Requisites Courses	Appointment type	Certificate Type	Notes
501	Pre-employment Police Training Course			None	Used to denote completion of the Pre-employment Police Training Course (Phase 1).
502	Pre-employment Basic Police Officer Equivalency	501 Pre-employment Police Training Course		MPTC	This code used to denote completion of Phase 2 of the Pre-employment Police Training Course in satisfaction of the police basic training requirements as established in section 209-q of the GML. ☐ MPTC Police Equivalency Certificate (071) issued.
503	Pre-employment Basic Police Officer Refresher	501 Pre-employment Police Training Course		MPTC	This code used to denote completion of Phase 2 of the Pre-employment Police Training Course in satisfaction of the police basic training requirements as established in section 209-q of the GML for students who have an expired transcript from a Pre-employment course (501). Eligible students have not exceeded ten years from date of issue of the transcript. MPTC Police Equivalency Certificate (071) issued.
504	Pre-employment Specialized Investigator Police Training - Equivalency		Prior Police Basic Training	MPTC	This code is used for pre-employment students who are hired by the Attorney General's Office as police investigators. Includes all pre-employment phase II units without SF-TR&O.
950	No Training Reported			None	
955	INVALID POLICE OFFICER BASIC TRAINING CERTIFICATE			None	To be used in the event NYS establishes a decertification of officers terminated for cause. This element of data nullifies the validity of basic training certificates for police and peace officers pursuant to GML §209-q (1)(c) and CPL §2.30(6).
957	INVALID PEACE OFFICER BASIC TRAINING CERTIFICATE			None	To be used in the event NYS establishes a decertification of officers terminated for cause. This element of data nullifies the validity of basic training certificates for police and peace officers pursuant to GML §209-q (1)(c) and CPL §2.30(6).

Appendix K

Table 5 - Learning Experiences (Continued)

Course Code	Course Name	Pre-Requisites Courses	Appointment type	Certificate Type	Notes
972	Initial Other Weapons Course - Aerosol Subject Restraint Equivalency		Appointed Peace	MPTC	This course will be used to identify peace officers that completed equivalent training while employed as a peace officer or police officer by an agency from out-of-state or with the federal government.
972	Initial Other Weapons Course - Baton Equivalency		Appointed Peace	MPTC	This course will be used to identify peace officers that completed equivalent training while employed as a peace officer or police officer by an agency from out-of-state or with the federal government.
972	Initial Other Weapons Course - Expandable Baton - Equivalency		Appointed Peace	MPTC	This course will be used to identify peace officers that completed equivalent training while employed as a peace officer or police officer by an agency from out-of-state or with the federal government.
977	Initial Firearms Course - Equivalency		Appointed Peace	MPTC	This course will be used to identify peace officers that completed equivalent training while employed as a peace officer or police officer by an agency from out-of-state or with the federal government.
978	NYPD School Safety Officer Course		Appointed NYPD School Safety Officer	MPTC	This course was approved by the MPTC on September 12, 2012, as satisfying the minimum training requirements for peace officers appointed as School Safety Agents by the New York City Police Department. It is not transferrable to other designations. (Registered as 27-Special Patrolman)
979	FDNY Fire Protection Inspector Course		Appointed FDNY Inspector	MPTC	This course was approved on 12/5/2012 for use by the FDNY in satisfaction of the peace officer training requirements for Fire Protection Inspectors. This course is not transferrable to other peace officer designations and is only approved for use by the FDNY. Courses delivered since June 2, 2011 using this standard are approved for certification.

Appendix K

Table 5 - Learning Experiences (Continued)

Course Code	Course Name	Pre-Requisites Courses	Appointment type	Certificate Type	Notes
980	FDNY Probationary Firefighter Course		Appointed FDNY Firefighter	MPTC	This course was approved on 12/5/2012 for use by the FDNY in satisfaction of the peace officer training requirements for Probationary Fire Firefighters. This course is not transferrable to other peace officer designations and is only approved for use by the FDNY. Courses delivered since June 2, 2011 using this standard are approved for certification.
981	Fundamentals of Probation Practice		Appointed Probation Officer	MPTC	Approved at June 1, 2011 MPTC meeting in satisfaction of the peace officer basic training requirement for persons appointed as probation officers. Does not contain firearms range training and is not transferrable to other designations of peace officer.
982	Basic Course for Parole Officers		Appointed Parole Officer	MPTC	Approved at June 1, 2011 MPTC meeting. Approved in satisfaction of peace officer basic training requirement for persons appointed as parole officers. Non-transferrable to other designations of peace officer.
983	Basic Course for Correction Officers - Equivalency		Appointed Correction Officer	MPTC	Created pursuant to amendment to Executive Law 840 and 841 giving MPTC /Commissioner authority over CO Training. ☐ 09/02/2009 MPTC approved 9 NYCRR 6108 Basic Course for Correction Officers including language regarding equivalencies for former NYS DOCS and NYC DOCS personnel effective 10/04/09. ☐ 10/04/09 Officers entered under this code will now receive 983 MPTC cert in satisfaction of both 9 NYCRR 6018 and 9 NYCRR 6025.
985	Direct Supervision for Line Staff	987 Basic Course for Correction Officer		DCJS	SCOC Required learning for facilities conducted with the Direct Supervision model.
986	Inmate Classification	987 Basic Course for Correction Officer		MPTC	Code activated pursuant to amendment to Executive Law 840 and 841 giving MPTC /Commissioner authority over CO Training. ☐

Appendix K

Table 5 - Learning Experiences (Continued)

Course Code	Course Name	Pre-Requisites Courses	Appointment type	Certificate Type	Notes
987	Basic Course for Correction Officers		Appointed Correction Officer	MPTC	Code reactivated pursuant to amendment to Executive Law 840 and 841 giving MPTC /Commissioner authority over CO Training.
988	Basic Course for Peace Officers - Equivalency		Prior Correction Officer Training	MPTC	Code used to denote completion of basic training which exceeds the Basic Course for Peace Officers to include a valid certificate for the Basic Course for Police Officers or its equivalent (Pre-employment/NYPD/NYSP).
992	Initial Other Weapons Course - Aerosol Subject Restraint		Appointed Peace Officer	MPTC	
992	Initial Other Weapons Course - Baton		Appointed Peace Officer	MPTC	
992	Initial Other Weapons Course - CED		Appointed Peace Officer	MPTC	This code created to capture completion of initial other weapons training for peace officers armed with a CED.
992	Initial Other Weapons Course - Expandable Baton		Appointed Peace Officer	MPTC	
993	Annual Other Weapons Course - Aerosol Subject Restraint		Appointed Peace Officer	None	
993	Annual Other Weapons Course - Baton		Appointed Peace Officer	None	
993	Annual Other Weapons Course - CED		Appointed Peace Officer	None	This code created to capture annual other weapons training for peace officers in the use of CEDs.
993	Annual Other Weapons Course - Expandable Baton		Appointed Peace Officer	None	
996	Annual Firearms Course		Appointed Peace Officer	None	
997	Initial Firearms Course		Appointed Peace Officer	None	
998	Basic Course for Peace Officers with Firearm		Appointed Peace Officer	MPTC	1/1/2011 - Amendment to CPL 2.30 made initial firearms applicable only for officers who are armed by the employer. After 6/2/2011, code is only used for general classifications of peace officer (not for county corrections, probation, parole, NYS DOCS -correction officers).

Appendix K

Table 5 - Learning Experiences (Continued)

Course Code	Course Name	Pre-Requisites Courses	Appointment type	Certificate Type	Notes
999	Basic Course for Peace Officers		Appointed Peace Officer	MPTC	

Table 6 - Registry Data Requirements (Continued)

The table below depicts the data required by DCJS to maintain the Registry. The specific data entry fields available to DCJS Staff via the current Ingenium System are noted in the "Data Name" column.

Item #	Data Name	Field Requirements	Comments
1	Employee ID	Unknown	Currently SSN- authorized by law to collect (Exec 845/POL 6-A)
2	Employee Name	Alpha >10 characters	Requires fields for first name, last name, middle initial, suffix
3	Employee Gender	Alpha 1 character or button	M/F
4	Employee D.O.B	Date mm/dd/yyyy	Additional identifier
5	Employee email	free text > 10 characters	For delivery of notifications and certifications
6	Employee Telephone	Telephone Number	For persons identified as agency contacts - personal/emergency numbers
7	Employee Weapon Indicator	Check box	Identifies which weapons (firearms, aerosol device, baton, CED, all, none, combination) are authorized to carry. Has implications on required training.
8	Employee Permit #	Numeric, 8 characters	For learners with NYS DOH breath analysis permit. Used/created by a partner agency.
9	Organization ID	Alphanumeric, 8 characters	Current configuration denotes agency type, county, number within the county
10	Organization Name	Alpha >10 Characters	Currently includes name and organization ID
11	Organization Address	Alphanumeric, >10 characters	
12	Organization City	Alpha, >10 Characters	
13	Organization State	Alpha, CAPS, 2 characters	
14	Organization Postal	Numeric, 10 characters	
15	Organization County	Alpha, > 10 characters	
16	Organization email	free text > 10 characters	For delivery of notifications and certifications
17	Organization Contact	Alpha >10 characters	Currently links to employee record and selects the CEO based on assigned role
18	Organization Telephone 1	Telephone Number	
19	Organization Telephone 2	Telephone Number	
20	Organization Facsimile	Telephone Number	
21	Organization URL	Alphanumeric, >10 characters	
22	Organization Note	Free Text, >10 characters	Captures specific data about the Organization
23	Emp. Org. History Status	Alpha, 1 character	F/P - Full or part-time
24	Emp. Org. History Start Date	Date mm/dd/yyyy	
25	Emp. Org. History End Date	Date mm/dd/yyyy	
26	Emp. Org. History Promo Date	Date mm/dd/yyyy	Captures effective dates for each promotion (i.e. sergeant, lieutenant, etc.)
27	Emp. Org. History Promo Date	Date mm/dd/yyyy	Captures job/role effective dates for each title (i.e. chief, training, registry, SWAT, etc.)
28	Date of last activity	mm/dd/yyyy	Indicate when an agency last accessed its registry
29	Emp. Org. History Title	Alpha (predefined list)	Learner may have multiple roles associated with a job. Police Officer, Deputy Sheriff, Correction Officer, Chief, Lieutenant, Sergeant, Instructor, SWAT, etc.... Required for registry (Exec. 845)

Appendix K

Table 6 - Registry Data Requirements (Continued)

Item #	Data Name	Field Requirements	Comments
30	Emp. Org. History Role	Alpha (predefined list)	Police Officer, Police Supervisor, Peace Officer, Campus Security Officer, Civilian
31	Emp. Org. History Primary	Alpha 1 character or button	Y/N
32	Emp. Org. History Criminal Procedure Law Designation	Numeric 3 character	Designation for police or peace officer title (0-99 and growing)
33	Learning Experience (courses) ID	Numeric, 3 characters	Course titles
34	Learning Experience Name	Alpha >10 characters	
35	Learning Experience Hours	Numeric, 4 characters	
36	Learning Experience Active	Alpha 1 character or button	Y/N
37	Event ID	Numeric	Current consists of Learning Exp. Code:2 digit zone, 2 digit location, 2 digit event #, 2digit year
38	Event Name	Link to Learning Experience Name	Course title
39	Event Start Date	Date mm/dd/yyyy	
40	Event End Date	Date mm/dd/yyyy	
41	Event Completed Date	Date mm/dd/yyyy	Some courses are filed as 1/1 - 12/31. Completed date indicates when each officer completed.
42	Event Note	Free Text, >10 characters	Captures specific data about an event
43	Event Certification period	Numeric, 4 characters	Durational validity for specific certifications
44	Event Pass/Fail	Alpha, 1 Character	Used to denote if the student was successful (S), unsuccessful (U), or incomplete (I).
45	Event Certification Date	Date mm/dd/yyyy	Calculates durational validity adding certification period to completion date
46	Skill ID	Numeric	
47	Skill Name	Alpha Numeric	Unique skill sets: Instructor, K-9 Handler, SWAT
48	Skill Certification Period	Numeric, 4 characters	Durational validity for specific Skills
49	Skill Name	Date mm/dd/yyyy	Calculates durational validity adding skill period to completion date
50	(SGP) School ID	Numeric, 8 characters	Sequential number indicating county of origin and number of school.
51	(SGP) School Name	Alpha >10 Characters	Currently includes name and School ID
52	(SGP) School Address	Alphanumeric, >10 characters	
53	(SGP) School City	Alpha, >10 Characters	
54	(SGP) School State	Alpha, CAPS, 2 characters	
55	(SGP) School Postal	Numeric, 10 characters	
56	(SGP) School County	Alpha, > 10 characters	
57	(SGP) School email	free text > 10 characters	For delivery of notifications and certifications
58	(SGP) School Contact	Alpha >10 characters	Requires fields for first name, last name, middle initial, suffix
59	(SGP) School Telephone1	Telephone Number	
60	(SGP) School Telephone2	Telephone Number	
61	(SGP) School Facsimile	Telephone Number	
62	(SGP) School URL	Alphanumeric, >10 characters	

Table 6 - Registry Data Requirements (Continued)

Item #	Data Name	Field Requirements	Comments
63	(SGP) School Notes	Free Text, >10 characters	Captures specific data about the School
64	(SGP) Facility ID	Numeric, 8 characters	Satellite location for approved SGP School
65	(SGP) Facility Name	Alpha >10 Characters	Linked to School Name
66	(SGP) Facility Address	Alphanumeric, >10 characters	
67	(SGP) Facility City	Alpha, >10 Characters	
68	(SGP) Facility State	Alpha, CAPS, 2 characters	
69	(SGP) Facility Postal	Numeric, 10 characters	
70	(SGP) Facility County	Alpha, > 10 characters	
71	(SGP) Facility email	free text > 10 characters	Linked to School Name
72	(SGP) Facility Contact	Alpha >10 characters	Linked to School Contact
73	(SGP) Facility Telephone1	Telephone Number	Linked to School Name
74	(SGP) Facility Telephone2	Telephone Number	
75	(SGP) Facility Facsimile	Telephone Number	
76	(SGP) Facility URL	Alphanumeric, >10 characters	Linked to School Name
77	(SGP) Facility Notes	Free Text, >10 characters	Captures specific data about the School
78	(SGP) Instructor ID	Numeric, 8 characters	Sequential number
79	(SGP) Instructor Name	Alpha >10 Characters	Currently includes name and School ID
80	(SGP) Instructor Address	Alphanumeric, >10 characters	
81	(SGP) Instructor City	Alpha, >10 Characters	
82	(SGP) Instructor State	Alpha, CAPS, 2 characters	
83	(SGP) Instructor Postal	Numeric, 10 characters	
84	(SGP) Instructor County	Alpha, > 10 characters	
85	(SGP) Instructor email	free text > 10 characters	For delivery of notifications and certifications
86	(SGP) Instructor Telephone1	Telephone Number	
87	(SGP) Instructor Schools	Numeric	Links to all schools (like employee organization history)
88	(SGP) Instructor Notes	Free Text, >10 characters	Captures specific data about the School
89	(SGP) Course Approval	Button	Issue approval of individual SGP course curricula
90	Accredited Agency	Button	Identify Accredited Agencies
91	Accreditation Date	Date mm/dd/yyyy	Date accreditation was issued
92	Accredited Agency maturity date	Date mm/dd/yyyy	Five years from accreditation
93	Reaccreditation Date	Date mm/dd/yyyy	Date reaccreditation was issued
94	Reaccredited Agency maturity date	Date mm/dd/yyyy	Five years from reaccreditation
95	Accreditation participating agency	Button	Agencies actively seeking accreditation
96	Accreditation participating agency date	Date mm/dd/yyyy	track length of process for agencies actively seeking accreditation

Appendix K

Table - 7 Skills and Roles

The table below depicts the current Ingenium interface allows DCJS staff to search the data base for records associated with a specific skill or role.

Item#	Skill or Role	Comments
1	Accredited Agency	Identifies Accredited Agencies
2	Accreditation Assessor	Identifies qualified accreditation assessors
3	Accreditation Program Manager	Identifies qualified accredited agency program managers
4	Accreditation participating agency	Identifies agencies actively seeking accreditation
5	Accreditation Council Members	Identifies members of the Law Enforcement Accredited Agency Council
6	Campus Security Officer	Prefer auto assignment based on Criminal Procedure Law designation - a "role"
7	Campus Department	Chief Executive of a campus safety organization
8	District Attorney	Prefer auto assignment based on Criminal Procedure Law designation - a "role"
9	Driving While Intoxicated	
10	Federal Excess Property Program	
11	Instructor Consultant	
12	Peace Officer	Prefer auto assignment based on Criminal Procedure Law designation - a "role"
13	Police Department	Chief Executive of a PD
14	Police Officer	Prefer auto assignment based on Criminal Procedure Law designation - a "role"
15	Probation Department	Probation Director
16	Sex Offender Registry	
17	Sheriff Department	Sheriff
18	State Police Zone	
19	Training Academies	Training Academy Director
20	Training Directors	Members of Training Director's Association (not always academy director)
21	TRIAD	Track membership on Committee for Coordination of Police Services to Elderly Persons
22	University - Police	Prefer auto assignment based on Criminal Procedure Law designation - a "role"

* May have more than one role at a time

Appendix K

Table 8 - Titles of Police and Peace Officers Used by the Registry

The table below depicts the current use of Job Titles for identifying Police & Peace Officers in the Registry. The corresponding Criminal Procedure Law designations of each officer is listed and serves as a Registry Code used by Ingenium to identify the titles.

Item #	Job Title	Criminal Procedure Law/ Registry (Ingenium) Code	Notes
1	Agent	7,53	Peace Officer: Defined in Appendix K, Table 9
2	Animal Control Officer	76,79	Peace Officer: Defined in Appendix K, Table 9
3	Assistant Chief	0	Police Officer Title CPL section 1.20(34)
4	Assistant Chief Fire Marshal	0,61,62,65,77	Police Officer Title CPL section 1.20(34) Peace Officer: Defined in Appendix K, Table 9
5	Assistant Chief Inspector	0	Police Officer Title CPL section 1.20(34)
6	Assistant Deputy Chief of Police	0	Police Officer Title CPL section 1.20(34)
7	Assistant Deputy Superintendent	0	Police Officer Title CPL section 1.20(34)
8	Assistant Fire Marshal	30	Peace Officer: Defined in Appendix K, Table 9
9	Auxiliary Police	26	Peace Officer: Defined in Appendix K, Table 9
10	Bay Constable	18	Peace Officer: Defined in Appendix K, Table 9
11	Bridge and Tunnel Officer	20	Peace Officer: Defined in Appendix K, Table 9
12	Captain	0, 21, 25	Police Officer Title CPL section 1.20(34)
13	Cell Block Attendant	64	Peace Officer: Defined in Appendix K, Table 9
14	Chief	0,21, 25	Police Officer Title CPL section 1.20(34)
15	Chief Fire Marshal	0,61,62,65,77	Peace Officer: Defined in Appendix K, Table 9
16	Chief Inspector	0	Police Officer Title CPL section 1.20(34)
17	Chief of Detectives	0	Police Officer Title CPL section 1.20(34)
18	Civilian	99	Peace Officer: Defined in Appendix K, Table 9
19	Commander	0	Police Officer Title CPL section 1.20(34)
20	Commissioner	99,81	Peace Officer: Defined in Appendix K, Table 9
21	Confidential Investigator	6	Peace Officer: Defined in Appendix K, Table 9
22	Constable	1	Peace Officer: Defined in Appendix K, Table 9
23	Corporal	0	Police Officer Title CPL section 1.20(34)
24	Correction Officer	25	Peace Officer: Defined in Appendix K, Table 9
25	Court Clerk	21	Peace Officer: Defined in Appendix K, Table 9
26	Court Officer	21,69,73,74,76,81	Peace Officer: Defined in Appendix K, Table 9
27	Court Security Officer	79,80,81	Peace Officer: Defined in Appendix K, Table 9
28	Deputy Inspector	0	Police Officer Title CPL section 1.20(34)
29	Deputy Marshal	21	Peace Officer: Defined in Appendix K, Table 9
30	Deputy Sheriff	0, 2	Police Officer Title CPL section 1.20(34) & Peace Officer: Defined in Appendix K.9

Appendix K
Table - 8 Titles of Police and Peace Officers Used by the Registry (Continued)

Item #	Job Title	Criminal Procedure Law/ Registry (Ingenium) Code	Notes
31	Deputy Superintendent	0,25	Police Officer Title CPL section 1.20(34)Peace Officer:Defined in Appendix K.9
32	Detective	0	Police Officer Title CPL section 1.20(34)
33	Detective Captain	0	Police Officer Title CPL section 1.20(34)
34	Detective Lieutenant	0	Police Officer Title CPL section 1.20(34)
35	Detective Sergeant	0	Police Officer Title CPL section 1.20(34)
36	Director	99	Peace Officer: Defined in Appendix K, Table 9
37	Dog Control Officer	56,68,75	Peace Officer: Defined in Appendix K, Table 9
38	Fire Inspector	30	Peace Officer: Defined in Appendix K, Table 9
39	Fire Marshal	0,30,61,62,65,71,77	Peace Officer Title CPL section 2.10 (multiple)
40	Fire Police	41	Peace Officer: Defined in Appendix K, Table 9
41	Fire Protection Inspectors	44	Peace Officer: Defined in Appendix K, Table 9
42	Firefighter	28	Peace Officer: Defined in Appendix K, Table 9
43	Harbor Master	19	Peace Officer: Defined in Appendix K, Table 9
44	Harbor Park Ranger	57	Peace Officer: Defined in Appendix K, Table 9
45	Inspector	0,8	Police Officer Title CPL section 1.20(34)Peace Officer:Defined in Appendix K.9
46	Inspector General	68	Peace Officer: Defined in Appendix K.9
47	Investigator	0,3,4,5,16,32,34,36,68	Police Officer Title CPL section 1.20(34)Peace Officer:Defined in Appendix K.9
48	Lieutenant	0,20,25	Police Officer Title CPL section 1.20(34)Peace Officer:Defined in Appendix K.9
49	Major	0, 25	Police Officer Title CPL section 1.20(34)Peace Officer:Defined in Appendix K.9
50	Marine Patrol Officer	68,70	Peace Officer: Defined in Appendix K, Table 9
51	Marshal	21,33	Peace Officer: Defined in Appendix K, Table 9
52	Officer	7,8,51,57-a,59,75	Peace Officer: Defined in Appendix K, Table 9
53	Park Ranger	9,10,11,57,57-a,74	Peace Officer: Defined in Appendix K, Table 9
54	Parole Officer	23	Peace Officer: Defined in Appendix K, Table 9
55	Parole Revocation Specialist	23	Peace Officer: Defined in Appendix K, Table 9
56	Patrolman	0,22,43	Police Officer Title CPL section 1.20(34)Peace Officer:Defined in Appendix K.9
57	Peace Officer	45,46,47,48,49,62,75,77,79,82	Peace Officer: Defined in Appendix K, Table 9
58	Police Officer	0	Police Officer Title CPL section 1.20(34)
59	Probation Officer	24	Peace Officer: Defined in Appendix K, Table 9
60	Seasonal Park Ranger	57a	Peace Officer: Defined in Appendix K, Table 9
61	Security Officer	17,52,63,66,67,68,72,78	Peace Officer: Defined in Appendix K, Table 9

Appendix K
Table - 8 Titles of Police and Peace Officers Used by the Registry (Continued)

Item #	Job Title	Criminal Procedure Law/ Registry (Ingenium) Code	Notes
62	Sergeant	0,20,25	Police Officer Title CPL section 1.20(34)Peace Officer:Defined in Appendix K.9
63	Sheriff	0	Police Officer Title CPL section 1.20(34)
64	Special Deputy Sheriff	42,74 a	Peace Officer: Defined in Appendix K, Table 9
65	Special Investigator	35,38	Peace Officer: Defined in Appendix K, Table 9
66	Special Officer	40	Peace Officer: Defined in Appendix K, Table 9
67	Special Patrolmen	27,37,39	Peace Officer: Defined in Appendix K, Table 9
68	Special Policeman	12,13,29,54	Peace Officer: Defined in Appendix K, Table 9
69	Supervising Fire Inspector	30	Peace Officer: Defined in Appendix K, Table 9
70	Transportation Supervisor	50	Peace Officer: Defined in Appendix K, Table 9
71	Trooper	0	Police Officer Title CPL section 1.20(34)
72	Undersheriff	0	Police Officer Title CPL section 1.20(34)
73	Warrant Officer	23	Peace Officer: Defined in Appendix K, Table 9
74	Deputy Assistant Water Superintendent	98 not a CPL code	Peace Officer: Defined in Appendix K, Table 9
75	Water Superintendent	98 not a CPL code	Peace Officer: Defined in Appendix K, Table 9
76	Watershed Inspector	98 not a CPL code	Peace Officer: Defined in Appendix K, Table 9

Appendix K

Table - 9 Peace Officer Designations

The below table lists the Criminal Procedure Law Section 2.10 designation and corresponding descriptions of Persons Designated as Peace Officers. This list expands and contracts as new designations are added and removed every year.

CPL 2.10	Descriptions of Persons Designated as Peace Officers as defined in Criminal Procedure Law Section 2.10
1	Constables or police constables of a town or village
2	The sheriff, undersheriff and deputy sheriffs of New York City and Sworn officers of the Westchester County department of public safety services appointed after January 31, 1983 to the title of public safety officer
3	Investigators of the office of the state commission of investigation
4	Employees of the department of taxation and finance
5	Employees of the New York City department of finance
6	Confidential investigators and inspectors of the department of agriculture and markets
7	Officers or agents of a duly incorporated society for the prevention of cruelty to animals
8	Inspectors and officers of the New York city department of health
9	Park rangers in Suffolk county
10	Park rangers in Broome county
11	Park rangers in Onondaga and Cayuga counties
12	Special policemen designated by the commissioner and the directors of in-patient facilities in the office of mental health and special policemen designated by the commissioner and the directors of facilities under his jurisdiction in the office of mental retardation and developmental disabilities
13	Persons designated as special policemen by the director of a hospital in the department of health
15	Uniformed enforcement forces of the New York state thruway authority
16	Employees of the department of health
17	Uniformed housing guards of the Buffalo municipal housing authority
18	Bay constable of the city of Rye, the villages of Mamaroneck, South Nyack and bay constables of the towns of East Hampton, Hempstead, Oyster Bay, Riverhead, Southampton, Southold, Islip, Shelter Island, Brookhaven, Babylon, Smithtown, Huntington and North Hempstead
19	Harbor masters appointed by a county, city, town or village
20	Bridge and tunnel officers, sergeants and lieutenants of the Triborough bridge and tunnel authority
21	Uniformed court officers, court clerks in the first and second departments, marshal, deputy marshal, clerk or uniformed court officer of a district court of the unified court system, marshals or deputy marshals of a city court, uniformed court officers of the city of Mount Vernon, and the city of Jamestown
22	Patrolmen appointed by the Lake George park commission
23	Parole officers or warrant officers or Parole revocation specialists in the department of corrections and community supervision
24	Probation officers

Table - 9 Peace Officer Designations (Continued)

CPL 2.10	Descriptions of Persons Designated as Peace Officers as defined in Criminal Procedure Law Section 2.10
25	Officials, as designated by the commissioner of the department of corrections and community supervision and correction officers of any state correctional facility or of any penal correctional institution
26	Peace officers designated pursuant to the provisions of the New York state defense emergency act
27	New York city special patrolmen appointed by the police commissioner
28	All officers and members of the uniformed force of the New York city fire department
29	Special policemen for horse racing
30	Supervising fire inspectors, fire inspectors, the fire marshal and assistant fire marshals of the county of Nassau fire marshal's office
32	Investigators of the department of motor vehicles
33	A city marshall of the city of New York who has received training in firearms handling from the federal bureau of investigation or in the New York city police academy, or in the absence of the available training programs from the federal bureau of investigation and the New York city police academy, from another law enforcement agency located in the state of New York
34	Waterfront and airport investigators
35	Special investigators appointed by the state board of elections
36	Investigators appointed by the state liquor authority
37	Special patrolmen of a political subdivision
38	A special investigator of the New York city department of investigation who has received training in firearms handling in the New York police academy and has received a firearms permit from the license division of the New York city police department.
39	Broome county special patrolman, appointed by the Broome county attorney
40	Special officers employed by the city of New York or by the New York city health and hospitals corporation
41	Fire police squads
42	Special deputy sheriffs appointed by the sheriff for Cornell university or any state institution constituting a part of the educational and research plants
43	Housing patrolmen of the Mount Vernon housing authority
44	The officers, employees and members of the New York city division of fire prevention, in the bureau of fire
45	Persons appointed and designated as peace officers by the Niagara frontier transportation authority
46	Persons appointed as peace officers by the Sea Gate Association
47	Employees of the department of financial services when designated as peace officers by the superintendent of financial services
48	New York state air base security guards when they are designated as peace officers under military regulations
49	Members of the army national guard military police and air national guard security personnel belonging to the organized militia of the state of New York when they are designated as peace officers under military regulations

Table - 9 Peace Officer Designations (Continued)

CPL 2.10	Descriptions of Persons Designated as Peace Officers as defined in Criminal Procedure Law Section 2.10
50	Transportation supervisors in the city of White Plains appointed by the commissioner of public safety in the city of White Plains
51	Officers and members of the fire investigation division of the fire department of the city of Rochester, the city of Binghamton and the city of Utica
52	Security hospital treatment assistants, as so designated by the commissioner of the office of mental health while transporting persons convicted of a crime to court, to other facilities within the jurisdiction of the office of mental health, or to any state or local correctional facility
53	Authorized agents of the municipal directors of weights and measures in the counties of Suffolk, Nassau and Westchester
54	Special policemen appointed pursuant to section one hundred fifty-eight of the town law
56	Dog control officers of the town of Brookhaven, who at the discretion of the town board may be designated as constables for the purpose of enforcing article twenty-six of the agriculture and markets law and for the purpose of issuing appearance tickets permitted under article seven of such law
57	Harbor Park rangers employed by the Snug Harbor cultural center in Richmond county and appointed as New York city special patrolman by the police commissioner
57a	Seasonal park rangers of the Westchester county department of public safety while employed as authorized by the commissioner of public safety/sheriff of the county of Westchester
57a	Officers of the Westchester county public safety emergency force, when activated by the commissioner of public safety/sheriff of the county of Westchester
58	Uniformed members of the security force of the Troy housing authority
59	Officers and members of the sanitation police of the department of sanitation of the city of New York, duly appointed and designated as peace officers by such department
61	Chief fire marshal, assistant chief fire marshal, fire marshal II and fire marshal I, all of whom are full-time employees of the Suffolk county department of fire, rescue and emergency services
62	Chief fire marshal, assistant chief fire marshal, fire marshal II and fire marshal I, all of whom are full-time employees of the town of Babylon, when acting pursuant to their special duties in matters arising under the laws related to fires, the extinguishment thereof and fire perils
62	Employees of the division for youth assigned to transport and warrants units who are specifically designated by the director
63	Uniformed members of the fire marshal's office in the town of Southampton and the town of Riverhead
63	Employees of the town court of the town of Greenburgh serving as a security officer
64	Cell block attendants employed by the city of Buffalo police department
65	Chief fire marshal, assistant chief fire marshal, fire marshal II and fire marshal I, all of whom are full-time employees of the town of Brookhaven, when acting pursuant to their special duties in matters arising under the laws related to fires, the extinguishment thereof and fire perils
66	Employees of the village court of the village of Spring Valley serving as security officers at such village court
67	Employees of the town court of the town of Putnam Valley serving as a security officer

Table - 9 Peace Officer Designations (Continued)

CPL 2.10 Descriptions of Persons Designated as Peace Officers as defined in Criminal Procedure Law Section 2.10	
68	Employees of the town court of the town of Southampton serving as uniformed court officers at such town court
68	The state inspector general and investigators designated by the state inspector general
68	Dog control officers of the town of Arcadia, who at the discretion of the town board may be designated as constables for the purpose of enforcing article twenty-six of the agriculture and markets law and for the purpose of issuing appearance tickets
68	Employees appointed by the sheriff of Livingston county, when acting pursuant to their special duties serving as uniformed marine patrol officers
68	Persons employed by the Chautauqua county sheriff's office serving as court security officers
69	Employees of the village court of the village of Amityville serving as uniformed court officers at such village court
70	Employees appointed by the sheriff of Yates county, pursuant to their special duties serving as uniformed marine patrol officers
71	Town of Smithtown fire marshalls when acting pursuant to their special duties in matters arising under the laws relating to fires, the extinguishment thereof and fire perils
72	Persons employed by Canisius college as members of the security force of such college
73	Employees of the town court of the town of Newburgh serving as uniformed court officers at such town court
74 a	Special duty sheriffs appointed by the sheriff of Tompkins county for the protection of Ithaca college
74	Employees of the village court of the village of Quogue, town of Southampton serving as uniformed court officers at such village court. Employees of the town court of the town of East Hampton serving as uniformed court officers at such town court
74	Parks and recreation forest rangers employed by the office of parks, recreation and historic preservation
75	Dog control officers of the town of Clarence, who at the discretion of the town board may be designated as constables for the purpose of enforcing article twenty-six of the agriculture and markets law for th purpose of issuing appearance tickets
75	Airport security guards, senior airport security guards, airport security supervisor, retired police officers, and supervisors of same, who are designated by resolution of the town board of the town of Islip to provide security at Long Island MacArthur Airport
75	Officers and members of the fire investigation unit of the fire department of the city of Buffalo
76	Employees of the village court of the village of Southampton, town of Southampton serving as uniformed court officers at such village court
76	Animal control officers employed by the city of peckskill
77	Chief fire marshal, assistant chief fire marshal, and fire marshals, all of whom are full-time employees of the town of East Hampton, when acting pursuant to their special duties in matters arising under the laws related to fires, the extinguishment thereof and fire perils
77	Syracuse University peace officers appointed by the chief law enforcement officer of the city of Syracuse
78	A security officer employed by a community college who is specifically designated as a peace officer by the board of trustees of a community college

Table - 9 Peace Officer Designations (Continued)

CPL 2.10	Descriptions of Persons Designated as Peace Officers as defined in Criminal Procedure Law Section 2.10
79	Court security officers employed by the Wayne county sheriff's office
79	Peace officers appointed by the city university of New York
79	Supervisors and members of the arson investigation bureau and fire inspection bureau of the office of fire prevention and control
79	Animal control officers employed by the city of Elmira, who at the discretion of the city council of the city of Elmira may be designated as constables for the purpose of enforcing article twenty-six of the agriculture and markets law
80	Employees of the Onondaga county sheriff's department serving as uniformed court security officers at Onondaga county court facilities
81	Members of the security force employed by Erie County Medical Center
81	Employees of the town of Riverhead serving as court officers at town of Riverhead court facilities
81	Employees of the town court of the town of Southold serving as uniformed court officers at such town court
81	Commissioners of and court officers in the department of public safety for the town of Rye
81	Employees of the town of Yorktown serving as court attendants at town of Yorktown court facilities
81	Employees of the Lewis county sheriff's department serving as uniformed court security officers at Lewis county court facilities
82	Employees of the NYC Business Integrity Commission designated as peace officers by the chairperson of such commission
83a	Security services officers employed by the University of Rochester who are designated as peace officers by the board of trustees of the University of Rochester
98	Watershed protection and enforcement officers appointed by the city of Peekskill. Criminal Procedure Law § 2.16
99	Any person other than those persons defined as Police Officers pursuant to Criminal Procedure Law § 1.20; and any person other than those persons defined as Peace Officers pursuant to Criminal Procedure Law § 2.10.

Appendix K

Table - 10 Police Officer Designations

The below table lists the Criminal Procedure Law Section 1.20(34) designation and corresponding descriptions of Persons Designated as Police Officers.

CPL 1.20(34) Descriptions of Persons Designated as Peace Officers as defined in Criminal Procedure Law Section 1.20(34)	
a.	A sworn member of the division of state police;
b.	Sheriffs, under-sheriffs and deputy sheriffs of counties outside of New York City;
c.	A sworn officer of an authorized county or county parkway police department;
d.	A sworn officer of an authorized police department or force of a city, town, village or police district;
e.	A sworn officer of an authorized police department of an authority or a sworn officer of the state regional park police in the office of parks and recreation;
f.	A sworn officer of the capital police force of the office of general services;
g.	An investigator employed in the office of a district attorney;
h.	An investigator employed by a commission created by an interstate compact who is, to a substantial extent, engaged in the enforcement of the criminal laws of this state;
i.	The chief and deputy fire marshals, the supervising fire marshals and the fire marshals of the bureau of fire investigation of the New York City fire department;
j.	A sworn officer of the division of law enforcement in the department of environmental conservation;
k.	A sworn officer of a police force of a public authority created by an interstate compact;
l.	Long Island railroad police.
m.	A special investigator employed in the statewide organized crime task force, while performing his assigned duties pursuant to section seventy-a of the executive law.
n.	A sworn officer of the Westchester county department of public safety services who, on or prior to June thirtieth, nineteen hundred seventy-nine was appointed as a sworn officer of the division of Westchester county parkway police or who was appointed on or after July first, nineteen hundred seventy-nine to the title of police officer, sergeant, lieutenant, captain or inspector or who, on or prior to January thirty-first, nineteen hundred eighty-three, was appointed as a Westchester county deputy sheriff.
o.	A sworn officer of the water-supply police employed by the city of New York, appointed to protect the sources, works, and transmission of water supplied to the city of New York, and to protect persons on or in the vicinity of such water sources, works, and transmission.
p.	Persons appointed as railroad policemen pursuant to section eighty-eight of the railroad law.

Table - 10 Police Officer Designations (Continued)

CPL 1.20(34)	Descriptions of Persons Designated as Peace Officers as defined in Criminal Procedure Law Section 1.20(34)
q.	An employee of the department of taxation and finance (i) assigned to enforcement of the taxes imposed under or pursuant to the authority of article twelve-A of the tax law and administered by the commissioner of taxation and finance, taxes imposed under or pursuant to the authority of article eighteen of the tax law and administered by the commissioner, taxes imposed under article twenty of the tax law, or sales or compensating use taxes relating to petroleum products or cigarettes imposed under article twenty-eight or pursuant to the authority of article twenty-nine of the tax law and administered by the commissioner or (ii) designated as a revenue crimes specialist and assigned to the enforcement of the taxes described in paragraph (c) of subdivision four of section 2.10 of this title, for the purpose of applying for and executing search warrants under article six hundred ninety of this chapter, for the purpose of acting as a claiming agent under article thirteen-A of the civil practice law and rules in connection with the enforcement of the taxes referred to above and for the purpose of executing warrants of arrest relating to the respective crimes specified in subdivision four of section 2.10 of this title.
r.	Any employee of the Suffolk county department of parks who is appointed as a Suffolk county park police officer.
s.	A university police officer appointed by the state university pursuant to paragraph 1 of subdivision two of section three hundred fifty-five of the education law.
t.	A sworn officer of the department of public safety of the Buffalo municipal housing authority who has achieved or been granted the status of sworn police officer and has been certified by the division of criminal justice services as successfully completing an approved basic course for police officers.
u.	Persons appointed as Indian police officers pursuant to section one hundred fourteen of the Indian law.
v.	Supervisor of forest ranger services; assistant supervisor of forest ranger services; forest ranger 3; forest ranger 2; forest ranger 1 employed by the state department of environmental conservation or sworn officer of the division of forest protection and fire management in the department of environmental conservation responsible for wild land search and rescue, wild land fire management in the state as prescribed in subdivision eighteen of section 9-0105 and title eleven of article nine of the environmental conservation law, exercising care, custody and control of state lands administered by the department of environmental conservation.

Appendix L

Conversion Plan

Entity Relationship Diagram

Intentionally Blank

Appendix L

Conversion Plan

Legacy Data Migration - Requirement

The existing application system uses an Oracle database to maintain all course, student, organizational and course history data. There are a total of 20 Oracle tables that contain data needed in the new system. It is expected that this existing data will be migrated and converted to the new database as provided by the chosen vendor. It is expected that this will include a commitment by existing State staff to provide assistance in data mapping and data quality review to ensure an accurate and complete conversion. Materials provided as part of this data conversion review will include a data dictionary and an entity-relationship diagram that will provide a primary description of how the existing data from the existing system is being stored as starting point for a detailed conversion specification to be developed by the selected vendor.

Please provide a detailed description of the methodology and approach you will take to convert and load existing legacy data to your solution. Describe what level of experience you have migrating customer legacy data to your system, please identify how many installations you have done this for.

If you have previous experience converting data from an Ingenium installation to your product please specify what version of Ingenium you worked with.

If you have a specified methodology for data conversion, specify how many times it has been used in the past.

Appendix M

Acceptance Testing Requirements

Intentionally Blank

Appendix M

Acceptance Testing Requirements

I. Background

Acceptance tests will be performed on the Public Safety Credentialing and Training System to determine if the system meets base system requirements specified within RFP Section 3.0, Attachments 7 and Attachment 8. These test plans shall be for all hardware, functionality and requirements including, but not limited to, all software, equipment and quality assurance processes. The State reserves the right to conduct additional functionality, interoperability, reporting, backup and restore and availability tests at any time during the life of the contract.

Acceptance test criteria will include, but not be limited to, validation of system functions against requirements, performance of the system against the mandatory base system requirements, how the system interoperates with State systems and how the system integrates with required integration points.

II. Acceptance Testing Requirements

- A. The Offerer/ Contractor shall prepare and document test plans, including expected results and validation techniques. These plans must be approved by NYS prior to acceptance testing and shall be contract deliverables.
- B. The Offerer/ Contractor and NYS shall perform acceptance testing.
- C. The Offerer/ Contractor shall provide a full and complete audit trail for all acceptance testing and the requisite reporting from this audit trail.
- D. The Contractor shall perform Load / Stress, Backup, Restore and Recovery testing prior to implementation.

This Page Intentionally Blank

Appendix N

NYS DCJS Technology Policy, June 4, 2007

DCJS Technology Policy

**Protection of NY State Division of
Criminal Justice Services' Information
Assets**

Issue Date: June 4, 2007

Publication Date: June 4, 2007

TABLE OF CONTENTS

TABLE OF CONTENTS.....	2
PURPOSE	4
SCOPE	4
POLICY STATEMENTS.....	5
PART 1. GENERAL STATEMENT OF MANAGEMENT INTENT	5
PART 2. INTRODUCTION TO INFORMATION RISK MANAGEMENT	5
PART 3. POLICY REQUIREMENTS	6
Section 1. Information Security Infrastructure	6
Section 2. Asset Classification.....	6
2.1 Information classification.....	6
2.2 Asset management.....	6
Section 3. Risk Management and Risk Analysis	7
3.1 Risk analysis.....	7
3.2 Security testing	7
Section 4. Business Use of Systems.....	7
4.1 Right to Monitor	7
4.2 Authorized Use Notice	7
4.3 Individual Use	7
Section 5. System and Information Availability	8
Section 6. Integrity of Data Processing Environment.....	8
Section 7. Protection of Information, Systems and Physical Infrastructure.....	8
7.1 Identification and Authentication	8
7.2 Access control	8
7.3 Physical and environmental security.....	9
7.4 Logical Security	9
7.5 Monitoring system use	10
7.6 Security Incident Procedures.....	10
7.7 Secure Disposal of Information.....	10
7.8 Confidentiality and Non-disclosure	10
Section 8. Implementation and Enhancements to Systems and Physical Infrastructure	10
Section 9. Virus and Malicious Software Prevention	11
9.1 Anti-virus software	11
9.2 Software Licenses and Copyrights.....	11
Section 10. Privacy.....	11
Section 11. Change Management	11
Section 12. Interconnectivity	12
12.1 Sharing Information Outside DCJS	12
12.2 Encryption	12
12.3 Network Connectivity	12
12.4 Internet.....	13
Section 13. User Training	13
PART 4. ROLES AND RESPONSIBILITIES	13
Section 1. Segregation of Duties and Supervision.....	13

DEFINITIONS.....	15
REQUIRED SUBMISSIONS AND NOTICES	17
COMPLIANCE	18
Section 1. Exceptions to Policy.....	18
ENFORCEMENT AND VIOLATION HANDLING	18
DOCUMENT CHANGE MANAGEMENT	18
Change History	18

PURPOSE

Ensuring the **integrity** and **confidentiality** of **information**, and the associated timely **availability** of **systems** to authorized **users** are the cornerstone of the New York State Division of Criminal Justice Services¹ (DCJS) ability to meet its customer service commitments. This policy details the responsibilities of the Agency **workforce** and all **third parties**. It is a statement of security responsibilities required of the DCJS **workforce** to establish and maintain an appropriately controlled and secure environment for DCJS **information** and the associated **systems** and **physical infrastructure**.

The primary objectives of this policy are:

- To establish and maintain a secure and reliable information processing foundation and a stable processing environment;
- To set forth methodologies to manage effectively the risk of security exposure or compromise within the DCJS **systems**;
- To promote understanding and compliance with all applicable laws and regulations; and
- To set forth a methodology for ongoing communication of this policy and compliance with this and associated policies.

These objectives will set forth a common set of security baselines and methodologies for all **users** of DCJS **systems**. Achieving these objectives will require supporting standards and associated guidelines/procedures. The DCJS Information Security Officer (ISO), in conjunction with relevant program units, will develop and implement these.

SCOPE

This policy is intended to protect any **systems**, **information**, or **physical infrastructure**, regardless of the form or format, created or used in support of DCJS.

It applies to:

- All members of the DCJS, Division of Probation and Correctional Alternatives (DPCA), the State Commission of Correction (SCOC) and Office for the Prevention of Domestic Violence (OPDV) **workforce**.
- **Third parties** as far as they access² any **systems**, **information**, or **physical infrastructure** created or used in support of DCJS.
- **Users** who access any systems, information, or physical infrastructure created or used in support of DCJS.

Implementation of the DCJS Security Program requires definition and resourcing by DCJS and its customer agencies. Publication of these Policies and Standards does not imply or warrant that all elements of the Security Program will be implemented where they have not been so defined or resourced by the customer.

DCJS reserves the right to remove access from DCJS workforce, third parties, or any user(s) whose activities or practices jeopardize the confidentiality, integrity, and availability of **DCJS systems**, **information**, or **physical infrastructure**.

¹ Also known as 'the Agency'

² Access shall mean physical or virtual use or entry.

POLICY STATEMENTS

Part 1. General Statement of Management Intent

Information is among DCJS's more valuable assets and DCJS relies upon information to support its business activities. The quality of preservation and retention of such **information** is key to DCJS's ability to provide services to its customers; the citizens of New York State; and to fulfill its statutory responsibilities. Therefore, the security of DCJS's **information** and of the technology that facilitates its use is a responsibility shared by all of DCJS. Any **user** who has been authorized to access DCJS **information** has an obligation to preserve and protect DCJS assets in a consistent and reliable manner. Controls, such as those set forth in this policy, provide the necessary physical and procedural safeguards to accomplish such obligations.

The establishment and management of such controls enable **information** to be shared while ensuring protection of that **information** and its associated **systems**. DCJS management, together with DCJS **workforce** and **third parties**, is responsible for ensuring that appropriate controls are in place to maintain the objectives of confidentiality, integrity, and availability for DCJS's **information**. However, every person with access to **information** is responsible for compliance with any and all security measures as a condition of being granted such access.

All **information** must only be used for its intended State purpose. **Information** must be appropriately protected from its creation, during its useful life, and through its authorized disposal. All **information** must be maintained in a secure, accurate, and reliable manner and be readily available for authorized use.

Compliance with applicable legislative and regulatory mandates are key elements of DCJS's Information Security program. Thus, all **information** will be processed, maintained and disposed of in accordance with all relevant federal and state laws, rules, and regulations. Any questions or concerns regarding Information Security should be addressed to the Information Security Officer (ISO) at (informationsecurityoffice@dcjs.state.ny.us) or through the Customer Contact Center.

Part 2. Introduction to Information Risk Management

To effectively secure DCJS and customer **information**, we must understand and address some fundamental questions:

- Do we know who is accessing **information** and **systems**?
- Can we control what they do?
- Can we ensure the integrity of the **information**?
- Can we prevent unauthorized changes to and deletions of **information**?
- Can we provide for non-repudiation of a transaction? (Can it be proved that someone performed a transaction?)
- Do we know what our customers' **system** availability requirements are and can we achieve them?

- Do we know:
 - If there is a problem?
 - Has the problem been identified soon enough to take appropriate action?
 - What actions must be taken to minimize/contain the problem?

This policy will help the Agency answer these questions and provide the basis for an effective and efficient operational environment. Compliance with this and associated policies, standards and guidelines/procedures constitutes sound business practice and will enable the Agency to ensure that **information** assets and **systems** are protected.

Part 3. Policy requirements

Section 1. Information Security Infrastructure

DCJS will establish a management framework to initiate and control the implementation of information security within the Agency. This management forum will approve the Information Security policy, assign security roles and coordinate the implementation of security across the Agency. As part of the Information Security Program, DCJS will appoint an Information Security Officer (ISO) and appropriately staff an Information Security function, to provide a focal point for managing information risk, including management, implementation, advice and compliance monitoring.

The ISO will report to the DCJS Chief Information Officer (CIO) and shall work with DCJS program units to ensure that information risks facing DCJS are:

- Understood;
- Managed in a consistent manner across the various DCJS program units; and
- Managed in a cost effective manner.

Section 2. Asset Classification

2.1 Information classification

Information must be classified and protected based on, among other factors, its sensitivity and criticality to DCJS customers, risks related to unauthorized disclosure thereof, and legal and/or regulatory requirements. As such, **information** must be classified in two respects:

Sensitivity: defines both how **confidential** the **information** is, and how 'sensitive' the **information** is to unauthorized changes (the **integrity** of the **information**);

Criticality: concerning the **availability** of **information**, being the ability for authorized **users** to access **systems** and **information** when required, without any interruptions.

All **information** is to be classified by the **information owner** and clearly labeled to signify what security measures are appropriate.

The security classification of the **information** is a fundamental way of understanding the different security requirements and defining how to handle those differences. Management is required to explain the information classification schema to all new and existing personnel under its supervision.

2.2 Asset management

An inventory of DCJS **systems** and **physical infrastructure** will be created. Based on this information, the ISO shall ensure that appropriate levels of protection, commensurate with the value and importance of the **systems** and **physical infrastructure**, are provided.

Section 3. Risk Management and Risk Analysis

3.1 Risk analysis

A formal risk analysis program will be implemented to determine the level of security controls required for DCJS **information** and associated **systems** and **physical infrastructure**. The risk analysis will be updated to ensure that changing environments, technologies, or **vulnerabilities** are considered. Additional security risk analyses will be performed as new projects are identified or in response to the discovery of a significant vulnerability.

The security risk analysis program will be performed under the auspices of the ISO.

3.2 Security testing

The security of critical **physical infrastructure** and **systems** must be routinely re-evaluated. The definition of 'critical' and the testing regime will be determined by the ISO, in conjunction with the **physical infrastructure/system** owner.

Section 4. Business Use of Systems

DCJS retains full copyright and intellectual property rights over all the information assets that it owns. This includes (but is not limited to) data, documents, programs and systems, wherever or however they may be stored. As such, DCJS **workforce** and **third parties** can only remove, copy or use DCJS **information** for non-work purposes with the written consent of their supervisor and the **information owner**.

Any use of DCJS systems requires management approval.

4.1 Right to Monitor

For several reasons, including DCJS's unique role in state government in ensuring the security of critical **information, users** have no legitimate expectation of privacy during any use of any DCJS **system** or **information**, even if a private password is issued or encryption is used. Any use, whether authorized or not, may be periodically and randomly monitored, intercepted, recorded, read, copied, accessed or captured in any manner including in real time, and used or disclosed in any manner, by authorized personnel without additional prior notice to **users**.

4.2 Authorized Use Notice

Users must be notified that unauthorized use of DCJS assets is not permissible and that DCJS's internal systems must only be used for conducting DCJS's business as authorized by DCJS management.

Thus, banner text, approved by Counsel of DCJS, will be displayed at all **system** entry points where a **user** initially signs on.

4.3 Individual Use

Individual accountability is required on all DCJS **systems**. Access to DCJS **systems** will only be provided through the use of an individually assigned unique **credential** (e.g. user-id and password). At the request of management, a unique **credential** shall be assigned to each **user** and a list of all current **credentials** shall be maintained. **Users** of DCJS **systems** must only access resources to which they are authorized by means of their **credential**. **Credentials** and the computer resources accessed thereby are to be monitored.

Users must **authenticate** themselves to the **system** or **network**. This is often performed using a password. **Authentication** tokens must be treated as confidential information, secured by the **user**, and must not be disclosed to any third person.

A **user** is responsible for all activity performed under their **credential**.

Section 5. System and Information Availability

Information must be readily available for authorized use. Appropriate technologies and processes must be developed and implemented to ensure the availability of all DCJS **information** and **systems**, regardless of platform or delivery channel. Availability timeframes for **systems** will be based on the **criticality** of the **information**, as defined by the **information owner**. (See section 2.1 Information Classification).

Backup and recovery schedules must be established and tested to verify they can meet the availability timeframes.

To ensure appropriate and timely back-up, all information should be stored on the DCJS LAN and not on individual workstations. Where this is not technically feasible, it is the responsibility of **users** to maintain adequate backups of data stored on the workstation local hard drive.

Section 6. Integrity of Data Processing Environment

Controls must be established and documented to ensure the validity, accuracy, completeness and timely processing throughout all stages of data processing, specifically: data inputs, outputs, storage and during the actual processing of the data. These include (but are not limited to):

- Receipt of non-DCJS **information**;
- Transmission of **information** to non-DCJS entities;
- Maintaining a record of data processing activities and any abnormalities;
- Production and dissemination of sensitive output;
- Media storage and disposal; and
- Restricting access to 'live' **information and** the 'production' environment.

Section 7. Protection of Information, Systems and Physical Infrastructure

The DCJS **workforce** and **third parties** are responsible for maintaining the confidentiality of the **information** regardless of the media upon which it is maintained. The measures necessary will be commensurate with the sensitivity of the **information**.

7.1 Identification and Authentication

All DCJS **systems** will authenticate the identity of **users** prior to allowing any access. All **users** will be identified to the **system** by a **credential**, comprising:

- Unique user-ID; and
- Method of **authentication**.

The level of **authentication** will be commensurate with the sensitivity of the **information** being accessed.

Authentication rules must be automatically enforced by the **system** being accessed.

7.2 Access control

Physical and logical access control mechanisms must be established to ensure **information, systems** and **physical infrastructure** are protected commensurate with their sensitivity, criticality and **vulnerabilities** or **threats** they face.

Access controls will:

- Support the security concepts of minimum necessary access to **systems/information** to perform an authorized task and a demonstrated business need-to-know the **information** being accessed;

- Be defined and limited in accordance with the **users'** job responsibilities;
- Be fully documented; and
- Be auditable.

Changes to access requirements must be documented and authorized:

- For **information**, this responsibility rests with the **information owner**. This will not only include determining and authorizing which **users** should have access, but also what those access privileges should be, e.g. read only ability, updating ability, deletion, etc.
- Access for other **system** components, e.g., to the network, e-mail, printers etc must be authorized by the **user's** supervisor.

Access entitlements will:

- Be traceable to the user-ID and assigned owner;
- Be reviewed and verified at least semi-annually; and
- Reflect changes in **workforce** and **third party** status within twenty-four (24) hours of the change. **DCJS management** is responsible for the access rights of the **workforce** and **third parties** under their supervision.

7.3 *Physical and environmental security*

Physical and environmental security controls must be implemented such that all **information** assets and **physical infrastructure** are secured from physical loss, destruction, modification, unauthorized access and environmental threats or hazards.

Typically these include:

- data centers and the environmental services that support them;
- wiring closets;
- servers;
- storage facilities for information or components; and
- cabling infrastructure.

7.4 *Logical Security*

Software mechanisms and processes must be implemented to ensure that **systems** and **information** can only be accessed by authorized individuals.

All **systems** and **information** will be protected from unauthorized access. The following access control restriction protocols should be considered and implemented as required by the sensitivity of the information:

- Individual users (user-based access);
- For individual functions/roles (role-based access);
- To specifically authorized records (context-based access).

Security products, functions and/or management processes commensurate with the sensitivity of the information will be implemented. This requirement includes non-production environments such as test and development systems. Such security requirements shall be documented and signed off by the **information owner** and ISO. (Also see Section 8. Implementation and Enhancements to Systems and Physical Infrastructure).

7.5 *Monitoring system use*

DCJS will establish event logging, response and management procedures to monitor **system** usage and help ensure that access is only by authorized persons for explicitly authorized activities. Within the limitations of technology, such processes are to be integrated across all **systems**.

Audit logs should be sufficient in detail to allow reconstruction of events if **system** compromise or malfunction occurs. Audit logs should be tamper-proof to ensure they remain intact should a **system** be compromised.

Segregation of duties will be maintained between those responsible for undertaking the review and those whose activities are being monitored.

The **business owner** (or designee) is responsible for ensuring that **system** monitoring requirements have been defined, implemented and tested prior to migration into the production environment.

Audit log retention periods will be clearly defined to meet both operational and security needs, as well as legal requirements. As such, retention periods shall be reviewed and approved annually.

7.6 *Security Incident Procedures*

Users must report any observed, attempted or suspected Security Incidents to the attention of the DCJS ISO, via a **supervisor** and/or Customer Contact Center, as quickly as possible.

7.7 *Secure Disposal of Information*

All **information** will be securely disposed of according to its sensitivity in an approved manner that renders the **information** useless unless otherwise governed by legislative or regulatory requirements.

Such disposal includes all items of equipment containing storage media, e.g., fixed hard disks. These must be checked to ensure that any **information** or licensed software is removed or overwritten prior to disposal.

7.8 *Confidentiality and Non-disclosure*

Personnel who are not state employees will not be permitted access to non-public **information** until an appropriate Confidentiality and Non-Disclosure Agreement (CNDA) has been executed. Additionally, the DCJS **workforce** must not disclose outside the Agency, information deemed confidential, restricted (or similar) that has been entrusted to it by other parties unless the originator of the information has provided advance approval of the disclosure and the receiving party has signed an approved CNDA.

The ISO's office will be the DCJS-authorized entity to draft, with Counsel Approval, and obtain all executed CNDAs and maintain the originals.

Section 8. Implementation and Enhancements to Systems and Physical Infrastructure

To ensure that DCJS **information** is effectively secured, it is vital that security and **privacy** requirements are considered and defined as part of the initial planning phase of projects, when the business requirements are being identified. **Failure to do so often results in implementation delays and/or expensive remediation.** Thus, it is the responsibility of the **business owner** to understand the DCJS security and **privacy** requirements and conduct a security review of all new **systems** (either purchased or developed) or any major enhancement to existing **systems** or **physical infrastructure** in conjunction with the ISO.

Control/security specifications, including **system** recovery criteria, will be based on a risk assessment and/or on the sensitivity and criticality of the **information** and **systems**. The **business owner** is responsible for ensuring that these specifications are defined, implemented and tested, *prior* to being placed into a production environment.

Section 9. Virus and Malicious Software Prevention

9.1 Anti-virus software

Virus detection software must be installed, regularly updated, and used to scan computers and media for viruses. All files from any external source must be checked for viruses before use on any DCJS computer.

9.2 Software Licenses and Copyrights

All software installed on any DCJS system must have a valid license. Licensed software shall not be copied or duplicated, except as explicitly permitted pursuant to the license terms and conditions and pre-approved by management. No programs from an external source (including the Internet), whether licensed or not, are to be personally obtained and/or installed on any DCJS equipment, whether owned or leased, unless authorized directly by the ISO, or indirectly by a process that has been approved by the ISO. Original license documents must be available for inspection on request.

Section 10. Privacy

The protection of the privacy of DCJS's **information** is of utmost importance. Privacy may also be required by federal and state laws, rules, and regulations. All DCJS **workforce** and **third parties** with access to personal information are required to respect the confidentiality of that personal information.

The collection and maintenance of other personal data, including **information** about employees, agents, organizations and business partners, must have the following characteristics:

- **Users** should receive clear and conspicuous notice of DCJS's data practices before any **information** is collected. Further, information must be used only for the stated purpose for which it is gathered;
- **Users** should have the opportunity to limit secondary uses of data which they provide;
- **Users** should be afforded a mechanism to contest inaccurate or incomplete data and data collectors should implement some means to verify the information they maintain;
- Data collectors will take reasonable steps to protect data integrity;
- There should be a mechanism in place to enforce privacy protections appropriate to the sensitivity of the information; and
- Data will only be kept for the amount of time required by law or regulations or as long as it remains relevant for its primary purpose, as defined by the **information owner**.

Section 11. Change Management

Changes to **information**, **systems** and **physical infrastructure**, particularly those impacting the production environment, must be strictly controlled. Inadequate control of changes is a common cause of system or security failures. DCJS will have an integrated change management process with formal management responsibilities and procedures covering:

- maintaining a record of individuals and their authorization levels;
- identification and recording of changes at all stages of the migration process;
- ensuring changes are formally submitted by authorized users (e.g. the **business owner**);
- communication of change details to all relevant persons;
- assessment of the potential impact of such changes, in particular relating to the operational/control environments and security;
- comprehensive testing of proposed changes;

- formal, documented, acceptance of the change prior to implementation in the production environment (Approvals will be required for all interested parties, including the **business owner**.);
- implementation plan including:
 - training;
 - revision to documentation and procedures;
 - migration plan to reduce the likelihood of impact to the production environment; and
 - 'back-out' plan identifying responsibilities for aborting and recovering from unsuccessful changes;
- procedures for 'emergency' changes.

All changes to the production environment will be performed through the change management process.

Section 12. Interconnectivity

The security of **information** must be maintained as it is transmitted across networks. **Information** can only be shared outside DCJS with the written consent of the **information owner**.

12.1 Sharing Information Outside DCJS

Non-public **information** can only be shared with the documented authorization of the **information owner**³, including a current, signed CNDA where necessary.

12.2 Encryption

Encryption must be used to protect **confidential information** as identified by the **information owner**.

12.3 Network Connectivity

Connections to DCJS networks must be performed in a secure manner to preserve the integrity of the network, confidentiality and integrity of **information** transmitted over that network, and the availability of the network. As such:

- Only equipment, software, tools or services provided by a **state government** entity, or approved by the ISO and the **network owner** shall be permitted access to any **system** or network.
- Only the **network owner** will be permitted to monitor operational data and security events. No unauthorized hardware or software shall be loaded, installed and/or activated on any DCJS computer, LAN system, or workstation without prior approval from the **network owner**.
- All connections of servers/communications equipment to an DCJS network must be approved by the **network owner**. Such connectivity must conform to this policy and the **network owner's** architectural standards and configuration requirements. All elements must be logged and monitored.
- The identification and **authentication** of the **user** attempting access will be verified prior to any connection being made.
- **Third party** connections must have a business justification for the network connection, including an assessment of the risk and any compensating controls that may be necessary. An authorized, duly appointed representative from the **third party** must: (i) agree to conform to the requirements of this policy and associated standards before the network connection is allowed; (ii) be advised of the confidential nature of the Information; and (iii) be responsible for any breach of this policy.

³ Unless authorized by legal counsel.

- Approval is required in advance to access **systems** from remote locations. All parties requesting remote access must be authorized directly by the ISO or indirectly by a process that has been approved by the ISO. All remote access must be logged and monitored.

12.4 Internet

The Internet allows citizens to more readily communicate with their government, and offers opportunities to facilitate their interfaces with the State. It also offers DCJS a more cost-effective way to implement its service delivery channels. However, the very openness that allows it to be a useful tool, also presents significant security vulnerabilities. To mitigate these, the following measures must be implemented:

- Where applications are accessed from the Internet, there is a requirement to logically separate and 'compartmentalize' the various system components to reduce the impact of any security intrusion. Conceptually, the approach is to provide a defense in depth, so that there is time to detect and respond to intruders before they are able to access and compromise **information** and **systems**. The following must be logically and physically (on different physical machines) segregated:
 - Web layer subsystems that typically provide the user interface;
 - Application layer subsystems, which provide the business logic and accesses the data;
 - DCJS internal systems and databases; and
 - Wherever possible, security subsystems, such as Access/Authentication engines (LDAP), Remote Authentication Servers, etc.
- All external Internet Protocol (IP) connections to an DCJS network are to be protected by an ISO- approved firewall.
- All external Internet connections to an DCJS network are to be protected by an ISO- approved real-time intrusion detection system.
- No updated or new DCJS Internet web page may go "live" without prior approval by the **information owner**, web master, and the DCJS CIO, or his or her designee with responsibility for public relations.

Section 13. User Training

All DCJS **workforce** with access to DCJS information will receive security awareness training to ensure they are knowledgeable about security procedures, their roles and responsibilities regarding the protection of DCJS information, and the proper use of information processing facilities to minimize security risks.

All new personnel will receive the awareness training and it will be reinforced annually for existing employees.

Part 4. Roles and Responsibilities

Section 1. Segregation of Duties and Supervision

Outlined below are key responsibilities for various categories of the DCJS **workforce**. This list does NOT include all security responsibilities, but is intended to provide an outline of roles and key responsibilities of DCJS workforce in safeguarding the Agency's data.

Function	Definition	Segregated duties ⁴	Key Security Responsibilities.
<i>DCJS management</i>	Any DCJS Supervisor or above.		- Know your role and responsibilities in the preparation and execution of your unit's Business Continuity Plan. - Ensure that your staff's computer access rights are accurate and up-to-date. In particular, inform the individual or organizational unit responsible for implementing amendments to user access rights of changes in staff roles/responsibilities, terminations and major leaves of absence within 24 hours. - Ensure that the staff within the unit are trained and understand their security responsibilities. - Inform ISO of all IT projects /major enhancements during the initial planning phase.
<i>Information owners</i>	Person(s) designated as 'owning' the data.		- Determine who should have access to protected resources within their jurisdiction, and what those access privileges should be (read only ability, updating ability, printing capacity, etc.). - Communicate to the ISO the requirements for protecting the data.
<i>Applications development</i>	DCJS workforce /vendor responsible for the development/enhancement of DCJS application software.	Operations, Network and communications, System Administration/ support, Data administration	- Inform ISO of all IT projects /major enhancements during the initial planning phase. - Ensure the integrity of the change management process: - There should be three discrete and distinct environments (development, user testing and production); - Non-development staff are responsible for migrating code between the environments; and - All changes are to be signed-off by the business owner before migration to production. - Ensure security requirements are incorporated in all developments/enhancements.
<i>Operations</i>	DCJS workforce responsible for the operations of a Consolidated State Datacenter mainframe/ server.	Applications development	- Know your role and responsibilities in the preparation and execution of an IT Disaster Recovery Plan for the site/facility. Part of this would include ensuring that back-up regime is sufficient to restore applications, data, and any system software/middleware. - Ensure computer/communications equipment is housed in locations with suitable physical and environmental controls. - Formalize and document operating procedures, including: - Instructions for job execution (scheduling, error handling, system restart, recovery etc); 'Housekeeping' such as shift/operator and fault logs; - Media handling, including storage, dissemination, transmission and disposal.
<i>Data administration</i>	DCJS workforce responsible for managing and maintaining DCJS data structures and data within (typically databases, but can be 'flat files')	Applications Development	Ensure that all changes to information are approved by the information owner.
<i>Network and communications</i>	DCJS workforce responsible for managing network infrastructure (e.g. data and phones)	Operations, Application Development	- Establish, implement and manage mechanisms for logging unauthorized attempts to use the network. - Implement a program and relevant tools to scan for security weaknesses (particularly for any components connected to the Internet or unauthorized usage of modems). - Document implementation guidelines, including security requirements, for network components and associated software. Instigate a process for ensuring that relevant 'patches' and other updates are implemented.
<i>System Administration/ support</i>	DCJS workforce responsible for managing a mainframe/ server.	Applications Development	- Document implementation guidelines (including security requirements) for servers and associated system software. Instigate a process for ensuring that relevant 'patches' and other updates are implemented. - Implement a program and relevant tools to scan for security weaknesses (particularly for any components connected to the Internet). - When responding to and resolving user problems, e.g. Help Desk or Workstation support) report

⁴ To reduce the **risk** of accidental or deliberate **system** misuse, separation of management or execution of certain duties or areas of responsibility must be implemented. This column defines which IT operational functions are incompatible with other functions, such as application development and IT operations. Where these cannot be achieved, a policy exemption must be applied for, and other compensatory **controls** such as monitoring of activities, audit trails and management supervision must be implemented

Function	Definition	Segregated duties ⁴	Key Security Responsibilities.
			any security breaches or non-compliance of policy to the ISO.
Information Security Officer (ISO)	Person designated as responsible for Information Security within DCJS	Operations, Application Development, Network and communications, System Administration/ support	• Represent DCJS in all Information security matters and shall coordinate and oversee security program activities and reporting processes in support of this policy and associated standards. • Liaison for all Information security matters between DCJS departments and facilities. • Maintain overall responsibility for ensuring the implementation, enhancement, monitoring and enforcement of this policy and associated standards.

DEFINITIONS

A complete listing of defined terms for NYS **Information** Technology Policies, standards, and Best Practice Guidelines is available in the [NYS Information Technology Policies, Standards, and Best Practice Guidelines Glossary \(http://www.oft.state.ny.us/policy/glossary.htm\)](http://www.oft.state.ny.us/policy/glossary.htm).

Terms defined for the first time in this policy are:

- Authentication.** Confirming a user's claim of identity. Dual factor (or strong authentication): An authentication scheme using two independent factors, e.g. something you know and something you have. Examples include the following:
- *Something you know:* user-id, passcode, memorized personal identification number (PIN) or password;
 - *Something you have:* something you own- an RSA secure authentication token, Smart card etc.; and
 - *Something you are:* biometrics, e.g., finger-print, retina scan.
- Availability** "Ensuring timely and reliable access to and use of information..." [44 U.S.C., SEC. 3542] A loss of **availability** is the disruption of access to or use of information or an information system.
- Business owner** Person who authorized the project, or a designated employee.
- Confidentiality** "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information..." [44 U.S.C., Sec. 3542] A loss of **confidentiality** is the unauthorized disclosure of information.
- Control** An action taken to enhance the likelihood that established goals or objectives will be achieved (in the context of this policy, generally an action taken to reduce **risk**.)
- Credential** An object that is verified when presented to the verifier in an authentication transaction. A common **credential** is a user-id and associated password.
- Encryption.** A technique to protect the **confidentiality** of **information**. The method transforms ("encrypts") readable **information** into unintelligible text through an algorithm and associated cryptographic key(s).
- Information** Any **information** created, stored in temporary or permanent form, filed, produced or reproduced by, regardless of the form or media. **Information** shall include, but not be limited to:
- Personally identifying **information**;
 - Reports, files, folders, memoranda;

- Statements, examinations, transcripts;
- Images; and
- Communications.

If information is already legally in the public domain (e.g. under FOIL), it can be considered as 'public' information. As such security controls are not required to maintain its confidentiality.

Information owner

An individual or organizational unit responsible for making classification and control decisions regarding use of information.

Integrity

"Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity..." [44 U.S.C., Sec. 3542] A loss of integrity is the unauthorized modification or destruction of information.

- *Authenticity* – A third party must be able to verify that the content of a message has not been changed in transit.
- *Non-repudiation* – The origin or the receipt of a specific message must be verifiable by a third party.
- *Accountability* - A security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.

Network owner

An individual or organizational unit responsible for operating and maintaining the physical and virtual infrastructure which comprises the network, including responsibility for establishing the procedures to be used for maintenance and upgrades.

Physical and environmental security

Measures taken to protect **systems** and **physical infrastructure** against threats associated with their physical environment. **Physical and environmental security** controls include the following broad areas:

- The facility's general geographic operating location determines the characteristics of *natural threats*, such as earthquakes and flooding; *man-made threats* such as burglary, civil disorders, or interception of transmissions and emanations; and *damaging nearby activities*, including toxic chemical spills, explosions, fires, and electromagnetic interference from emitters, such as radars.
- Supporting facilities are those services, both technical and human, that underpin the operation of the system. The system's operation usually depends on supporting facilities such as electric power, heating and air conditioning, and telecommunications. The failure or substandard performance of these facilities may interrupt operation of the system and may cause physical damage to system hardware or stored data.

Physical Infrastructure

A generic description of any area containing non end-user IT equipment and subsidiary hardware, e.g.:

- Mainframes;
- Servers;
- Communications equipment;
- Printing facilities;
- Media libraries; and
- Wiring closets.

Privacy

The right of individuals to determine for themselves when, how and to what extent information about them is communicated to others.

Risk	A risk is defined as where there are inadequate controls to mitigate a threat or vulnerability effectively. There are two elements to determine the import of a risk: • Impact- health and safety, reputational, legal and regulatory, financial, etc.; • Likelihood- likely to occur daily, weekly, etc.
Supervisor	An individual responsible for day-to-day management or supervision of a User .
System	An interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, applications, and communications.
Third parties the (Non-DCJS workforce)	Anyone directly, or indirectly providing goods and services to DCJS who is <u>not</u> under direct control of the Agency (see workforce below).
Threat	The potential for a person, object, or event to negatively impact the security of the physical infrastructure, systems or information. Threats can be malicious, such as the intentional modification of sensitive information, or they can be accidental, such as an error in a calculation, or the accidental deletion of a file. Threats can also be acts of nature, e.g., flooding, wind or lightning, etc. Other threats include: • Hacking; • Inability to access the datacenter; • Denial of service; • Loss of key staff; • Virus; • Data corruption; • Destruction of assets.
User	Any person authorized by the information owner to access the system for a legitimate governmental purpose
Vulnerabilities	Weaknesses in a system, application, or operating environment that can be exploited by a threat . For example, unauthorized access (the threat) to a system or application could occur by an outsider guessing an obvious password. The vulnerability exploited is an easily guessable password chosen by a user. Reducing or eliminating the vulnerabilities can reduce or eliminate the risk to the system, application, or data. For example, a tool that can help users choose robust passwords may reduce the chance that they will choose readily guessable passwords and thus reduce the threat of unauthorized access.
Workforce	State employees, and other persons whose conduct, in the performance of work for DCJS, is under the direct control of DCJS, whether or not they are paid by the Agency. In the policy, DCJS personnel or DCJS employees shall mean anyone in the DCJS workforce.

REQUIRED SUBMISSIONS AND NOTICES

None

COMPLIANCE

Compliance with this policy is mandatory. Roles and responsibilities will be addressed immediately after hiring, included in employment or other third-party contractual arrangements with users, and monitored during an individual's affiliation with DCJS. All employees, agents or other third parties who uses or otherwise has access to **information** must understand their roles and responsibilities regarding information security issues, including without limitation, protecting DCJS's **information** assets. Any non-compliance with this policy that results in the compromise of **information** confidentiality, integrity and/or availability may result in disciplinary action, up to and including termination, and/or possible prosecution under applicable local, state, and federal laws. DCJS will take every step necessary, to protect the security of its information assets.

Section 1. Exceptions to Policy

Exceptions to the policy must be approved in writing. A case describing the reason and timeframes for the exception must be documented in writing and submitted for approval to the ISO. If approved, the exception will be kept on file by the ISO. Waiver of any provision of this policy may be granted on a time-limited basis and for a single situation.

ENFORCEMENT AND VIOLATION HANDLING

Any compromise or suspected compromise of this policy must be reported to the appropriate management and the ISO. All violations of security policies and/or standards are subject to appropriate disciplinary action.

DOCUMENT CHANGE MANAGEMENT

Anyone in DCJS can request a modification to this policy. Recommendations for changes to this policy must be communicated in writing to the ISO. Upon receipt, the ISO shall review the request. If the ISO approves the change, the ISO shall revise this policy accordingly and communicate the revisions to management. Each manager shall be responsible for communicating the changes to persons under their supervision. Once in effect, new policies will be distributed.

The ISO is responsible for monitoring changes to the DCJS policy on Information Security and revising this policy and related documents. The policy will be reviewed to assess:

- the policy's effectiveness, demonstrated by the nature, number and impact of recorded security incidents;
- cost and impact of controls on business efficiency;
- effects of changes to technology.

The ISO reserves the right to modify this policy at any time with reasonable notice to applicable persons.

Obsolete copies of this document should be destroyed by the document holder as soon as is practical.

Change History

Only the changes introduced in the most recent version are itemized.

Changes to document:

- None

This Page Intentionally Blank

Appendix O

Enterprise Information Security Policy v4.0

Intentionally Blank



ANDREW M. CUOMO
Governor

STATE OF NEW YORK
State Capitol P.O. Box 2062
Albany, NY 12220-0062
www.its.ny.gov

BRIAN DIGMAN
NYS Chief Information Officer
Director, Office of IT Services

New York State Information Technology Policy	No: NYS-P03-002
IT Policy Name: Information Security	Updated: 06/20/2014
	Issued By: NYS ITS State Chief Information Officer Policy Owner: Enterprise Information Security Office

1.0 Purpose and Benefits of the Policy

This policy defines the mandatory minimum information security requirements for all State Entities (SE). Any SE may, based on its individual business needs and specific legal and federal requirements, exceed the security requirements put forth in this document, but must, at a minimum, achieve the security levels required by this policy.

This policy acts as an umbrella document to all other Office of Information Technology Services' (ITS) security policies and associated standards. This policy defines the responsibility of all SEs to:

- protect and maintain the confidentiality, integrity and availability of information and related infrastructure assets;
- manage the risk of security exposure or compromise;
- assure a secure and stable information technology (IT) environment;
- identify and respond to events involving information asset misuse, loss or unauthorized disclosure;
- monitor systems for anomalies that might indicate compromise; and
- promote and increase the awareness of information security.

Failure to secure and protect the confidentiality, integrity and availability of information assets in today's highly networked environment can damage or shut down systems that operate critical infrastructure, financial and business transactions and vital government functions; compromise data; and result in legal and regulatory non-compliance.

This policy benefits SEs by defining a framework that will assure appropriate measures are in place to protect the confidentiality, integrity and availability of New York State (NYS) data; and assure staff and all other affiliates understand their role and responsibilities, have adequate knowledge of security policy, procedures and practices and know how to protect SE information.

2.0 Enterprise IT Policy Statement

Section 2 of Executive Order No. 117 provides the State Chief Information Officer, who also serves as director of the NYS Office of Information Technology Services (ITS), the authority to oversee, direct and coordinate the establishment of information technology policies, protocols and standards for State government, including hardware, software, security and business re-engineering. Details regarding this authority can be found in NYS ITS Policy NYS-P08-002, Authority to Establish State Enterprise Information Technology (IT) Policy, Standards and Guidelines.

Except for terms defined in this policy, all terms shall have the meanings found in <http://www.its.ny.gov/policy/glossary.htm>.

3.0 Scope of the Policy

This policy applies to all “State government entities,” as defined in NYS Executive Order 117, staff and all other affiliates (e.g., contractors, vendors, solution providers), which have access to or manage SE information.

This policy encompasses all systems, automated and manual, for which New York State has administrative responsibility, including systems managed or hosted by third parties on behalf of the SE. It addresses all information, regardless of the form or format, which is created or used in support of business activities of SEs.

4.0 Policy Statement

4.1 Organizational Security

- a. Information security requires both an information risk management function and an information technology security function. Depending on the structure of the SE, an individual or group can serve in both roles or a separate individual or group can be designated for each role. It is recommended that these functions be performed by a high level executive or a group that includes high level executives.
 1. Each SE must designate an individual or group to be responsible for the risk management function assuring that:
 - i. risk-related considerations for individual information systems, including authorization decisions, are viewed from the perspective of the SE as an enterprise with regard to the overall strategic goals and objectives of the SE in carrying out its core missions and business functions; and
 - ii. the management of information system-related security risks is consistent across the SE, reflects the risk tolerance of the SE, and is considered along with other types of risks, in order to ensure mission/business success.

2. Each SE must designate an individual or group to be responsible for the technical information security function. For purposes of clarity and readability, this policy will refer to the individual, or group, designated as the Information Security Officer (ISO)/designated security representative. This function will be responsible for evaluating and advising on information security risks. For SEs that receive IT services as a member of one of the clusters within the Office of Information Technology Services (ITS), the information security function will be fulfilled by the Enterprise Information Security Office (EISO) and Cluster Security Services Teams.
- b. Information security risk decisions must be made through consultation with both function areas described in a. above.
 - c. Although the technical information security function may be outsourced to third parties, each SE retains overall responsibility for the security of the information that it owns.

4.2 Functional Responsibilities

- a. SE executive management is responsible for:
 1. evaluating and accepting risk on behalf of the SE;
 2. identifying SE security goals and integrating them into relevant processes;
 3. supporting the consistent implementation of information security policies and standards;
 4. supporting security within the SE through clear direction and demonstrated commitment of appropriate resources;
 5. promoting awareness of information security best practices through the regular dissemination of materials provided by the ISO/designated security representative;
 6. implementing the process for determining information classification and categorization, based on industry recommended practices, State directives, and legal and regulatory requirements, to determine the appropriate levels of protection for that information;
 7. determining who, within the SE, will be assigned and serve as information owners while maintaining ultimate responsibility for the confidentiality, integrity, and availability of the data;
 8. participating in the response to security incidents;
 9. complying with notification requirements in the event of a breach of private information;
 10. adhering to specific legal and regulatory requirements related to information security;
 11. communicating legal and regulatory requirements to the ISO/designated security representative; and
 12. communicating requirements of this policy and the associated standards, including the consequences of non-compliance, to the SE workforce and third parties, and addressing adherence in third party agreements.
- b. The ISO/designated security representative is responsible for:
 1. maintaining familiarity with SE business functions and requirements;

2. maintaining an adequate level of current knowledge and proficiency in information security through annual Continuing Professional Education (CPE) credits directly related to information security;
 3. assessing SE compliance with information security policies and legal and regulatory information security requirements;
 4. evaluating information security risks and assisting the SE in understanding its information security risks and how to appropriately manage those risks;
 5. representing and assuring security architecture considerations are addressed;
 6. advising on security issues related to procurement of products and services;
 7. escalating security concerns that are not being adequately addressed according to the applicable reporting and escalation procedures;
 8. disseminating threat information to appropriate parties;
 9. participating in the response to potential security incidents;
 10. participating in the development of enterprise policies and standards for NYS that consider SE needs; and
 11. promoting information security awareness.
- c. IT management is responsible for:
1. supporting security by providing clear direction and consideration of security controls in the data processing infrastructure and computing network which support the information owners;
 2. providing resources needed to maintain a level of information security control consistent with this policy;
 3. identifying and implementing all processes, policies and controls relative to security requirements defined by the SE's business and this policy;
 4. implementing the proper controls for information owned by the SE based on the SE's classification designations;
 5. providing training to appropriate technical staff on secure operations (e.g., secure coding, secure configuration);
 6. fostering the participation of information security and technical staff in protecting information assets, and in identifying, selecting and implementing appropriate and cost-effective security controls and procedures; and
 7. implementing business continuity and disaster recovery plans.
- d. The SE workforce is responsible for:
1. protecting State information and resources;
 2. abiding by the [Acceptable Use for Information Technology Resources Policy](#); and
 3. reporting suspected information security incidents or weaknesses to the appropriate manager and ISO/designated security representative.
- e. The Enterprise Information Security Office (EISO) is responsible for:
1. providing in-house expertise as security consultants to the SEs as needed;
 2. developing the State's security program and strategy, including measures of effectiveness;
 3. establishing and maintaining enterprise information security policy and standards;
 4. assessing SE compliance with security policies and standards;
 5. advising on secure system engineering;

6. providing incident response coordination and expertise;
7. monitoring the State networks for anomalies;
8. maintaining ongoing contact with security groups/associations and relevant authorities;
9. providing timely notification of current threats and vulnerabilities; and
10. providing awareness materials and training resources.

Associated Standard: [Continuing Professional Education Requirements for ISOs/Designated Security Representatives Standard](#)

4.3 Separation of Duties

- a. To reduce the risk of accidental or deliberate system misuse, separation of duties and areas of responsibility must be implemented where appropriate.
- b. Whenever separation of duties is not technically feasible, other compensatory controls must be implemented, such as monitoring of activities, audit trails and management supervision.
- c. The audit and approval of security controls must always remain independent and segregated from the implementation of security controls.

4.4 Information Risk Management

- a. Any system or process that supports SE business functions must be appropriately managed for information risk and undergo information risk assessments, at a minimum annually, as part of its life cycle.
- b. Information security risk assessments are required for new projects, implementations of new technologies, significant changes to the operating environment, or in response to the discovery of a significant vulnerability.
- c. SEs are responsible for selecting the risk assessment approach they will use based on their needs and any applicable laws, regulations, and policies.
- d. Risk assessment results, and the decisions made based on these results, must be documented.

Associated Standard: [Risk Management Standard](#)

4.5 Information Classification and Handling

- a. All information, which is created, acquired or used in support of SE business activities, must only be used for its intended business purpose.
- b. All information assets must have an information owner established within the SE's lines of business.

- c. Information must be properly managed from its creation, through authorized use, to proper disposal.
- d. All information must be classified on an ongoing basis based on its confidentiality, integrity and availability characteristics.
- e. An information asset must be classified based on the highest level necessitated by its individual data elements.
- f. If the SE is unable to determine the confidentiality classification of information or the information is Personal, Private, or Sensitive Information (PPSI), the information must have a high confidentiality classification and, therefore, is subject to high confidentiality controls.
- g. Merging of information which creates a new information asset or situations that create the potential for merging (e.g., backup tape with multiple files) must be evaluated to determine if a new classification of the merged data is warranted.
- h. All reproductions of information in its entirety must carry the same confidentiality classification as the original. Partial reproductions need to be evaluated to determine if a new classification is warranted.
- i. Each classification has an approved set of baseline controls designed to protect these classifications and these controls must be followed.
- j. The SE must communicate the requirements for secure handling of information to its workforce.
- k. A written or electronic inventory of all SE information assets must be maintained.
- l. SE content made available to the general public must be reviewed according to a process that will be defined and approved by the SE. The process must include the review and approval of updates to publicly available content and must consider the type and classification of information posted.
- m. PPSI must not be made available without appropriate safeguards approved by the SE.
- n. For non-public information to be released outside an SE or shared between SEs, a process must be established that, at a minimum:
 - 1. evaluates and documents the sensitivity of the information to be released or shared;
 - 2. identifies the responsibilities of each party for protecting the information;
 - 3. defines the minimum controls required to transmit and use the information;
 - 4. records the measures that each party has in place to protect the information;
 - 5. defines a method for compliance measurement;
 - 6. provides a signoff procedure for each party to accept responsibilities; and
 - 7. establishes a schedule and procedure for reviewing the controls.

Associated Standards: [Information Classification Standard](#); [Information Security Controls Standard](#); [Sanitization/Secure Disposal Standard](#)

4.6 IT Asset Management

- a. All IT hardware and software assets must be assigned to a designated business unit or individual.
- b. SEs are required to maintain an inventory of hardware and software assets, including all system components (e.g., network address, machine name, software version) at a level of granularity deemed necessary for tracking and reporting. This inventory must be automated where technically feasible.
- c. Processes, including regular scanning, must be implemented to identify unauthorized hardware and/or software and notify appropriate staff when discovered.
- d. All SE-owned IT hardware assets that have the potential to store, transport or transmit SE data must be labeled with an SE inventory tag.

Associated Standard: [Secure Configuration Standard](#)

4.7 Personnel Security

- a. The SE workforce must receive general security awareness training, to include recognizing and reporting insider threats, within 30 days of hire. Additional training on SE specific security procedures, if required, must be completed before access is provided to specific SE sensitive information not covered in the general security training. All security training must be reinforced at least annually and must be tracked by the SE.
- b. An SE must require its workforce to abide by the [NYS Acceptable Use of IT Resources Policy](#). An auditable process must be in place for users to acknowledge that they agree to abide by the [NYS Acceptable Use of IT Resources Policy](#).
- c. All job positions must be evaluated by the SE to determine whether they require access to sensitive information and/or sensitive information technology assets.
- d. For those job positions requiring access to sensitive information and sensitive information technology assets, SEs must conduct workforce suitability determinations, unless prohibited from doing so by law, regulation or contract. Depending on the risk level, suitability determinations may include, as appropriate and permissible, evaluation of criminal history record information or other reports from federal, state and private sources that maintain public and non-public records. The suitability determination must provide reasonable grounds for the SE to conclude that an individual will likely be able to perform the required duties and responsibilities of the subject position without undue risk to the State.
- e. A process must be established within the SE to repeat or review suitability determinations periodically and upon change of job duties or position.

- f. SEs are responsible for ensuring all State issued property is returned prior to an employee's separation and accounts are disabled and access is removed immediately upon separation.

Associated Standard: [Account Management/Access Control Standard](#)

4.8 Cyber Incident Management

- a. All observed or suspected information security incidents or weaknesses are to be reported to appropriate management and the ISO/designated security representative as quickly as possible. If a member of the workforce feels that cyber security concerns are not being appropriately addressed, they may confidentially contact the NYS Cyber Incident Response Team (CIRT) directly.
- b. The NYS CIRT must be notified of any cyber incident which may have a significant or severe impact on operations or security, or which involves digital forensics, to follow proper incident response procedures and guarantee coordination and oversight.
- c. Incident response procedures, consistent with New York State standards, must be clearly identified to promote effective response to security incidents.

Associated Standard/Procedure: [Cyber Incident Response Standard](#), [Cyber Incident Reporting Procedure](#)

4.9 Physical and Environmental Security

- a. Information processing and storage facilities must have a defined security perimeter and appropriate security barriers and access controls.
- b. A periodic risk assessment must be performed for information processing and storage facilities to determine whether existing controls are operating correctly and if additional physical security measures are necessary. These measures must be implemented to mitigate the risks.
- c. Information technology equipment must be physically protected from security threats and environmental hazards. Special controls may also be necessary to protect supporting infrastructure and facilities such as electrical supply and cabling infrastructure.
- d. All information technology equipment and information media must be secured to prevent compromise of confidentiality, integrity, or availability in accordance with the classification of information contained therein.
- e. Visitors to information processing and storage facilities, including maintenance personnel, must be escorted at all times.

Associated Standard: [Risk Management Standard](#)

4.10 Account Management and Access Control

- a. All accounts must have an individual employee or group assigned to be responsible for account management. This may be a combination of the business unit and information technology (IT).
- b. Except as described in the [Account Management/Access Control Standard](#), access to systems must be provided through the use of individually assigned unique identifiers, known as user-IDs.
- c. Associated with each user-ID is an authentication token (e.g., password, key fob, biometric) which must be used to authenticate the identity of the person or system requesting access.
- d. Automated techniques and controls must be implemented to lock a session and require authentication or re-authentication after a period of inactivity for any system where authentication is required. Information on the screen must be replaced with publically viewable information (e.g., screen saver, blank screen, clock) during the session lock.
- e. Automated techniques and controls must be implemented to terminate a session after specific conditions are met as defined in the [Account Management/Access Control Standard](#).
- f. Tokens used to authenticate a person or process must be treated as confidential and protected appropriately.
- g. Tokens must not be stored on paper, or in an electronic file, hand-held device or browser, unless they can be stored securely and the method of storing (e.g., password vault) has been approved by the ISO/designated security representative.
- h. Information owners are responsible for determining who should have access to protected resources within their jurisdiction, and what those access privileges should be (read, update, etc.).
- i. Access privileges will be granted in accordance with the user's job responsibilities and will be limited only to those necessary to accomplish assigned tasks in accordance with SE missions and business functions (i.e., least privilege).
- j. Users of privileged accounts must use a separate, non-privileged account when performing normal business transactions (e.g., accessing the Internet, e-mail).
- k. Logon banners must be implemented on all systems where that feature exists to inform all users that the system is for SE business or other approved use consistent with SE policy, and that user activities may be monitored and the user should have no expectation of privacy.

- l. Advance approval for any remote access connection must be provided by the SE. An assessment must be performed and documented to determine the scope and method of access, the technical and business risks involved and the contractual, process and technical controls required for such connection to take place.
- m. All remote connections must be made through managed points-of-entry reviewed by the ISO/designated security representative.
- n. Working from a remote location must be authorized by SE management and practices which assure the appropriate protection of SE data in remote environments must be shared with the individual prior to the individual being granted remote access.

Associated Standards: [Account Management/Access Control Standard](#), [Authentication Tokens Standard](#), [Identity Assurance Standard](#), [Remote Access Standard](#), [Security Logging Standard](#)

4.11 Systems Security

- a. Systems include but are not limited to servers, platforms, networks, communications, databases and software applications.
 - 1. An individual or group must be assigned responsibility for maintenance and administration of any system deployed on behalf of NYS. A list of assigned individuals or groups must be centrally maintained.
 - 2. All systems must be developed, maintained and decommissioned in accordance with a [secure system development lifecycle \(SSDLC\)](#).
 - 3. Each system must have a set of controls commensurate with the classification of any data that is stored on or passes through the system.
 - 4. All system clocks must synchronize to a centralized reference time source set to UTC (Coordinated Universal Time) which is itself synchronized to at least three synchronized time sources.
 - 5. Environments and test plans must be established to validate the system works as intended prior to deployment in production.
 - 6. Separation of environments (e.g., development, test, quality assurance, production) is required, either logically or physically, including separate environmental identifications (e.g., desktop background, labels).
 - 7. Formal change control procedures for all systems must be developed, implemented and enforced. At a minimum, any change that may affect the production environment and/or production data must be included.
- b. Databases and Software (including in-house or third party developed and commercial off the shelf (COTS):
 - 1. All software written for or deployed on SE systems must be free from common coding vulnerabilities and resilient to high-risk threats before being deployed in production.
 - 2. Once test data is developed, it must be protected and controlled for the life of the testing in accordance with the classification of the data.

3. Production data may be used for testing only if a business case is documented and approved in writing by the information owner and the following controls are applied:
 - i. All security measures, including but not limited to access controls, system configurations and logging requirements for the production data are applied to the test environment and the data is deleted as soon as the testing is completed; or
 - ii. sensitive data is masked or overwritten with fictional information.
4. Where technically feasible, development software and tools must not be maintained on production systems.
5. Where technically feasible, source code used to generate an application or software must not be stored on the production system running that application or software.
6. Scripts must be removed from production systems, except those required for the operation and maintenance of the system.
7. Privileged access to production systems by development staff must be restricted.
8. Migration processes must be documented and implemented to govern the transfer of software from the development environment up through the production environment.

c. Network Systems:

1. Connections between systems must be authorized by the executive management of all relevant SEs and protected by the implementation of appropriate controls.
2. All connections and their configurations must be documented and the documentation must be reviewed by the information owner and the ISO/designated security representative annually, at a minimum, to assure:
 - i. the business case for the connection is still valid and the connection is still required; and
 - ii. the security controls in place (filters, rules, access control lists, etc.) are appropriate and functioning correctly.
3. A network architecture must be maintained that includes, at a minimum, tiered network segmentation between:
 - i. Internet accessible systems and internal systems;
 - ii. systems with high security categorizations (e.g., mission critical, systems containing PPSI) and other systems; and
 - iii. user and server segments.
4. Network management must be performed from a secure, dedicated network.
5. Authentication is required for all users connecting to State internal systems.

6. Network authentication is required for all devices connecting to State internal networks.
7. Only SE authorized individuals or business units may capture or monitor network traffic.
8. A risk assessment must be performed in consultation with the SE ISO/designated security representative before the initiation of, or significant change to, any network technology or project, including but not limited to wireless technology.

Associated Standards: [Secure System Development Lifecycle Standard](#), [Secure Coding Standard](#), [Security Logging Standard](#), [Secure Configuration Management Standard](#)

4.12 Vulnerability Management

- a. All systems must be scanned for vulnerabilities before being installed in production and periodically thereafter.
- b. All systems are subject to periodic penetration testing.
- c. Penetration tests are required periodically for all critical environments/systems.
- d. Where a SE has outsourced a system to another SE or a third party, vulnerability scanning/penetration testing must be coordinated.
- e. Scanning/testing and mitigation must be included in third party agreements.
- f. The output of the scans/penetration tests will be reviewed in a timely manner by the system owner. Copies of the scan report/penetration test must be shared with the ISO/designated security representative for evaluation of risk.
- g. Appropriate action, such as patching or updating the system, must be taken to address discovered vulnerabilities. For any discovered vulnerability, a plan of action and milestones must be created, and updated accordingly, to document the planned remedial actions to mitigate vulnerabilities.
- h. Any vulnerability scanning/penetration testing must be conducted by individuals who are authorized by the ISO/designated security representative. The EISO must be notified in advance of any such tests. Any other attempts to perform such vulnerability scanning/penetration testing will be deemed an unauthorized access attempt.
- i. Anyone authorized to perform vulnerability scanning/penetration testing must have a formal process defined, tested and followed at all times to minimize the possibility of disruption.

4.13 Operations Security

- a. All information processing facilities must have documented operating instructions, management processes and formal incident management procedures related to information security matters which define roles and responsibilities of affected individuals who operate or use information processing facilities.
- b. System configurations must follow approved configuration standards.
- c. Advance planning and preparation must be performed to ensure the availability of adequate capacity and resources. System capacity must be monitored on an ongoing basis.
- d. Where an SE provides a server, application or network service to another SE(s), operational and management responsibilities must be coordinated by all impacted SEs.
- e. Host based firewalls must be installed and enabled on all SE workstations to protect from threats and to restrict access to only that which is needed
- f. Controls must be implemented (e.g., anti-virus, software integrity checkers) across SE systems where technically feasible to prevent and detect the introduction of malicious code or other threats.
- g. Controls must be implemented to disable automatic execution of content from removable media.
- h. Controls must be implemented to limit storage of SE information to SE authorized locations.
- i. Controls must be in place to allow only SE approved software to run on a system and prevent execution of all other software.
- j. All systems must be maintained at a vendor-supported level to ensure accuracy and integrity.
- k. All security patches must be reviewed, evaluated and appropriately applied in a timely manner. This process must be automated, where technically possible.
- l. Systems which can no longer be supported or patched to current versions must be removed.
- m. Systems and applications must be monitored and analyzed to detect deviation from the access control requirements outlined in this policy and the [Security Logging Standard](#), and record events to provide evidence and to reconstruct lost or damaged data.
- n. Audit logs recording exceptions and other security-relevant events must be produced, protected and kept consistent with SE record retention schedules and requirements.

- o. Monitoring systems must be deployed (e.g., intrusion detection/prevention systems) at strategic locations to monitor inbound, outbound and internal network traffic.
- p. Monitoring systems must be configured to alert incident response personnel to indications of compromise or potential compromise.
- q. Contingency plans (e.g., business continuity plans, disaster recovery plans, continuity of operations plans) must be established and tested regularly. At a minimum, these plans must include:
 - 1. An evaluation of the criticality of systems used in information processing (including but not limited to software and operating systems, firewalls, switches, routers and other communication equipment).
 - 2. Recovery Time Objectives (RTO)/Recovery Point Objectives (RPO) for all critical systems.
- r. Backup copies of SE information, software, and system images should be taken regularly in accordance with SE defined requirements.
- s. Backups and restoration must be tested regularly. Separation of duties must be applied to these functions.
- t. Procedures must be established to maintain information security during an adverse event. For those controls that cannot be maintained, compensatory controls must be in place.

Associated Standards: [Secure Configuration Management Standard](#), [Security Logging Standard](#), [Incident Response Standard](#), [Account Management/Access Control Standard](#)

4.14 Citizens' Cyber Security Notification

- a. All SEs are required to notify an individual when there has been or is reasonably believed to have been a compromise of the individual's private information in compliance with [State Technology Law, Article II, Internet Security and Privacy Act](#).
- b. Beyond the requirements of the Act, SEs must also notify non-residents when there has been or is reasonably believed to have been a compromise of the individual's private information.
- c. This policy also applies to information maintained on behalf of an SE by a third party.
- d. The SE must consult with the EISO to help determine the scope of the breach and restoration measures.

5.0 Policy Compliance

This policy shall take effect upon publication. The Policy Unit shall review the policy at least once every year to ensure relevancy. The Office may also assess agency compliance with this policy.

To accomplish this assessment, ITS may issue, from time to time, requests for information to covered agencies, which will be used to develop any reporting requirements as may be requested by the NYS Chief Information Officer, the Executive Chamber or Legislative entities.

If compliance with this policy is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, SEs shall request an exception through the Enterprise Information Security Office [exception process](#).

Any violations of this policy and its associated standards may result in disciplinary action, civil penalties, and/or criminal prosecution. The SE will review alleged violations of this policy on a case-by-case basis and pursue recourse, as appropriate.

6.0 Definitions of Key Terms

Criticality	The degree to which an SE depends on the information or information system for the success of a mission or of a business function.
Wireless Technology	Technology that permits the transfer of information between separated points without physical connection. Currently wireless technologies use infrared, acoustic, radio frequency, and optical.
Penetration Testing	Test of the overall strength of an SE's defenses (technology, processes, people) by simulating the objectives and actions of an attacker.
Breach	Acquiring of information by a person without valid authorization or through unauthorized acquisition.
Private Information	As defined in State Technology Law, shall mean personal information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired: (1) social security number; (2) driver's license number or non-driver identification card number; or (3) account number, credit or debit card number, in combination with any required security code, access code, or password which would permit access to an individual's financial account. Private information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

7.0 ITS Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

Policy Owner
Attention: Enterprise Information Security Office
New York State Office of Information Technology Services
1220 Washington Avenue – Bldg. 7A, 4th Floor
Albany, NY 12242
Telephone: (518) 242-5200
Facsimile: (518) 322-4976

Questions may also be directed to your ITS Customer Relations Manager at:
Customer.Relations@its.ny.gov

The State of New York Enterprise IT Policies may be found at the following website:
<http://www.its.ny.gov/tables/technologypolicyindex.htm>

8.0 Review Schedule and Revision History

Date	Description of Change	Reviewer
04/18/2003	Original Policy Release (<i>released under the Office of Cyber Security and Critical Infrastructure Coordination (CSCIC)</i>)	
06/20/2014	Full revision	Deborah A. Snyder, Acting Chief Information Security Officer
06/20/2014	Scheduled policy review	

9.0 Related Documents

- [National Institute of Standards and Technology \(NIST\) Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations](#)
- International Standard ISO/IEC 27002, Information Technology – Security Techniques – Code of Practice for Information Security Controls
- [SANS Institute, Critical Security Controls for Effective Cyber Defense \(“Top 20 Critical Security Controls”\)](#)
- [State Technology Law, Article II, Internet Security and Privacy Act](#)

Appendix P

NYS OITS Data Center Services

Intentionally Blank



ITS Data Center Services

1. Purpose

This document describes the ITS Data Center Services that include Infrastructure, Platform, Integration and Common Application Services. These services will be delivered through a service catalog and will be available to Data Center Service Subscribers to host business application solutions.

2. Supported Environments

ITS provides support for a wide-range of environments to ensure that NYS programs have flexibility when identifying potential solutions for its business requirements.

Supported environments are as follows:

a) Operating Systems

- IBM POWER AIX
- Red Hat Enterprise Linux
- Microsoft Windows Server

b) Database (RDBMS)

- Oracle
- MS SQL
- DB2

c) Web Servers

- Apache
- Microsoft IIS
- IBM HTTP
- RedHat HTTP

d) Application Servers

- J2EE
 - i) WebSphere Application Server
 - ii) JBOSS
 - iii) Oracle WebLogic
- .NET - - Microsoft IIS

e) Authentication and Authorization Services

This service is based on LDAP and supports SAML and Netegrity SiteMinder to access the NYS Statewide Directory.

f) Mainframe Services - - z/OS and z/Linux

g) Virtual Server - - any application to be hosted by ITS must be able to run effectively within a virtual server environment running on an approved operating system (see above).

3. Service Catalog

The ITS service catalog will provide standardized infrastructure service bundle options, support and costs. The ITS service catalog process will drive governance and provisioning of services. ITS will work with the service consumer to assist in selecting the appropriate services to meet the solution's requirements as well as adherence to standards required for servers administered by the Data Center. These specifications will be based on service offerings that align with business service classifications for Critical, Important and Utility workloads:

1. Business Critical: High downtime impact - Critical real-time application with revenue, legal or ethical requirements for availability
2. Business Important: Moderate downtime impact – Real-time or near-time application which would materially affect revenue or service if unavailable
3. Business Utility: Low downtime impact – Applications which normally schedule or could schedule as outage

Service bundles will be available in varying sizes to fit the initial sizing of compute, memory and storage needs of the customers. Workloads will be monitored and right sized based on actual utilization over time.

4. Infrastructure Services:

The ITS Data Center Infrastructure Services are modeled around a fully managed infrastructure that includes standard hardware, software and support components.

Infrastructure Services include the following:

1. Operating Environments
2. Servers
3. Storage
4. Data Recovery
5. Data Replication

I. Infrastructure Services Capabilities:

1. Hosted in a primary Tier 3+ rated data center facility and an available DR facility for offsite backup and DR requirements
2. Highly performing and resilient networks – both IP and Storage networks
3. Local and global network load-balancing
4. System isolation will be available based on data classification, compliance and security requirements
5. Security controls such as anti-virus and DLP services
6. Infrastructure monitoring and alerting for all service components
7. Infrastructure security event monitoring and auditing
8. Based on a shared service model that is highly resilient, secure, and low latency for a broad set of system and business requirements
9. Highly virtualized at all layers of the infrastructure stack
10. Service management – Service catalog, Request, incident, change, problem and configuration management for all service components

II. Storage Services:

1. Block Storage Services with local and remote data protection
2. File Storage Services with local and remote data protection
3. Fixed Content / Object Storage Services – geographically distributed

5. Integration Services: Under development

6. Application Services: Under development

7. Shared Enterprise Application Services Standards:

I. Enterprise authentication and authorization service

This service is based on LDAP and supports SAML and Netegrity SiteMinder to access the NYS Statewide LDAP Directory.

II. Example Services Under Development

1. Enterprise Secure Managed File Transfer Service
2. Mapping and GIS services
3. Enterprise Service Bus
4. Document Management
5. Analytics Platform

Appendix Q

**Web Based Forms Supporting
NYS / DCJS Business Requirements**

Intentionally Blank

New York State Division of Criminal Justice Services
POLICE OFFICER REGISTRY ENTRY FORM - CERTIFICATION OF INITIAL EMPLOYMENT
(Executive Law § 845)

THIS FORM IS USED TO REGISTER A POLICE OFFICER WITH THE DIVISION OF CRIMINAL JUSTICE SERVICES. **USE THIS FORM FOR ALL INITIAL APPOINTMENTS AND TRANSFERS.** FORMS PRESENTED FOR FILING MUST CONTAIN ORIGINAL SIGNATURES. ALTHOUGH THE BLANK FORM MAY BE DUPLICATED, PHOTOCOPIES OF COMPLETED FORMS, OR FORMS WITH PHOTOCOPIED SIGNATURES WILL NOT BE ACCEPTED.

Pursuant to Executive Law §845, police officer employers are required to register police officers with the Division of Criminal Justice Services (DCJS). DCJS uses the police registry to determine an individual's eligibility to receive a police training certificate, and for other lawful purposes. DCJS reserves the right to require further documentation as necessary to properly classify a registrant. The information provided may be added to the registry and made available pursuant to law.

SECTION I: REGISTRANT INFORMATION

This section must be completed by the police officer registrant. Only individuals appointed to positions defined in Criminal Procedure Law §1.20(34) are eligible for registration.

If you were previously employed as a police officer in the State of New York, please circle "Yes" then proceed with completing the remainder of Section I. Officers previously employed as police officers in the State of New York who possess a **valid** certificate of completion for a Municipal Police Training Council approved Basic Course for Police Officers are not required by law or regulation to repeat police basic training. Validity of a certificate of completion is governed by General Municipal Law §209-q. This does not preclude an employer from requiring any appointee to attend police basic training.

Type or print legibly, the registrant's last name, first name, middle initial, date of birth, gender and Social Security Number. Enter the home mailing address, county of residence, home street address (if different) of the registrant. Temporary addresses are not acceptable. If the registrant is temporarily living away from home (e.g. enrolled at a college or university, on military assignment, etc.) **DO NOT** list the temporary address. Enter the registrant's city/state/country of birth (if other than U.S.). Registrants not born in the United States **MUST** include a certified copy of one of the following: (1) naturalization papers; (2) Department of State Birth certificate; or (3) currently valid United States Passport. Carefully read the certification. Sign and date in the area provided. Incomplete submissions will not be processed.

Pursuant to the New York State Personal Privacy Protection Law, DCJS is authorized to collect personal identifying information as part of a public safety agency record. Personal identifying information on this form shall not be revealed, released, transferred, disseminated or otherwise communicated orally, in writing, or by electronic means other than to the registrant. Disclosure of personal identifying information is voluntary, and refusal to provide personal identifying information shall not result in the denial of any right, benefit, or privilege.

SECTION II: AGENCY INFORMATION

Unless a written agreement is on file with DCJS, this section must be completed by the Chief Law Enforcement Officer (Chief, Sheriff, Director) of the appointing authority. The Executive Law mandates that all police officers must be registered with the Division of Criminal Justice Services. The information in Section II identifies the law enforcement agency with which the registrant is a police officer.

Type, or print legibly, the chief law enforcement officer's last name, first name, middle initial and title. Enter the name, telephone number (including area code) and address of the law enforcement agency. Indicate whether the appointment is full-time or part-time, whether background and residency checks were conducted, and if fingerprints were submitted to DCJS. Carefully read the certification. Sign and date in the area provided. All the information in Section II is required. When signing this section, the CEO is verifying their responsibility to

New York State Division of Criminal Justice Services
POLICE OFFICER REGISTRY ENTRY FORM - CERTIFICATION OF INITIAL EMPLOYMENT
(Executive Law § 845)

provide the registrant with the requisite basic training pursuant to General Municipal Law §209-q. Incomplete submissions will not be processed.

SECTION III: CIVIL SERVICE INFORMATION

The appropriate civil service commission officer must complete this section for all registrants, both full and part time. Civil Service Law mandates that the appointment of officers to the police force of a police department or police district must meet certain requirements. The information in Section III describes the registrant's appointment.

Type or print legibly, the civil service officer's last name, first name, middle initial and title. Enter the name, telephone number (including area code) and address of the civil service commission. Enter the job title and civil service classification of the person named in Section I. This should be the specific title/classification to which the registrant was appointed and that appears on the agency payroll. Carefully read the certification. Sign and date in the area provided. The information in Section III is required. Incomplete submissions will not be processed.

SECTION IV: OATH OF OFFICE

This section must be completed by the appropriate registrar/recorder of oaths of office. The Public Officers' Law mandates that every officer take and file an oath of office. The Information in Section IV indicates the date the oath was taken by the registrant, the place of filing, and title of the office.

Type or print legibly, the registrar/recording officer's last name, first name, middle initial and title. Enter the name, telephone number (including area code) and address of the registrar's/recorder's office. Enter the date the person named in Section I took and filed the oath of office for the position to which he or she was appointed with the agency named in Section II. Indicate the title of the office to which the registrant was sworn (e.g. police officer, deputy sheriff, etc). The oath of office date is the date recorded by DCJS as the appointment date of the officer. Carefully read the certification. Sign and date in the area provided. The information in Section IV is required. Incomplete submissions will not be processed.

MAILING INSTRUCTIONS

Mail completed forms to:

NYS Division of Criminal Justice Services
Alfred E. Smith State Office Building
Office of Public Safety – Records Unit
80 South Swan St., 3rd Floor
Albany, NY 12210

QUESTIONS

If you have any questions regarding this form, call (518) 485-1092 for assistance.

New York State Division of Criminal Justice Services
POLICE OFFICER REGISTRY ENTRY FORM - CERTIFICATION OF INITIAL EMPLOYMENT
(Executive Law § 845)

New York State Division of Criminal Justice Services
POLICE OFFICER REGISTRY ENTRY FORM - CERTIFICATION OF INITIAL EMPLOYMENT
 (Executive Law § 845)

SECTION I – REGISTRANT INFORMATION (To be completed by the registrant)

Were you previously a police officer in NYS? Yes No Police Officer as defined by NYS Criminal Procedure Law §1.20.	Last Name	First Name	MI	Date of Birth	Gender M F	Social Security Number*
	Home Residence Mailing Address		City, State, Zip			County of Home Residence
	Home Residence Street Address (if Different)		City, State, Zip			City, State, Country of birth (if other than U.S.)
I am the person named above. I understand that the information in Section I is part of a written statement that will be presented to the Division of Criminal Justice Services for filing, and I certify that it is true to the best of my knowledge and belief.						
Signature						Date

*Pursuant to the New York State Personal Privacy Protection Law, DCJS is authorized to collect personal identifying information as part of a public safety agency record. Personal identifying information on this form shall not be revealed, released, transferred, disseminated or otherwise communicated orally, in writing, or by electronic means other than to the registrant. Disclosure of personal identifying information is voluntary. Refusal to provide personal identifying information shall not result in the denial of any right, benefit, or privilege.

SECTION II – AGENCY INFORMATION (To be completed by the chief law enforcement officer)

Last Name	First Name	MI	Title of Person Signing Section II
Name of Law Enforcement Agency			Telephone
Address		City, State, ZIP	
Type of Appointment Full-time Part-time	Background Check Conducted Yes No	Residency Verified Yes No	Fingerprints submitted to DCJS Yes No
I am the chief law enforcement officer responsible for appointing the person named in Section I as a police officer of the above named law enforcement agency. I understand that the information in Section II is part of a written statement that will be presented to the Division of Criminal Justice Services for filing, and I certify that it is true to the best of my knowledge and belief. I understand I am responsible for providing the registrant with the requisite training pursuant to §209-q of the General Municipal Law.			
Signature			Date

SECTION III – CIVIL SERVICE INFORMATION (To be completed by the civil service officer for all registrants Full or Part-time)

Last Name	First Name	MI	Title of Person Signing Section III
Name of Civil Service or Personnel Agency			Telephone
Address		City, State, ZIP	
Title and Civil Service Classification of the Registrant			
I am the civil service officer responsible for certifying the appointment of individuals appearing on the payroll of the law enforcement agency named in Section II. I understand that the information in Section III is part of a written statement that will be presented to the Division of Criminal Justice Services for filing, and I certify that it is true to the best of my knowledge and belief.			
Signature			Date

SECTION IV – OATH OF OFFICE (To be completed by the registrar responsible for recording oaths of office)

Last Name	First Name	MI	Title of Person Signing Section IV
Name of Recording Office			Telephone
Address		City, State, ZIP	
Oath of Office Date	Oath of Office Title of the Registrant		
I am the officer responsible for recording the oaths of office of individuals appointed as police officers of the law enforcement agency named in Section II. The person named in Section I has filed an oath of office as a police officer, pursuant to an appointment received from the person named in Section II. I understand that the information in Section IV is part of a written statement that will be presented to the Division of Criminal Justice Services for filing, and I certify that it is true to the best of my knowledge and belief.			
Signature			Date

New York State Division of Criminal Justice Services
POLICE OFFICER REGISTRY UPDATE FORM
 (Executive Law § 845)

Page of Pages

1. Agency Name:		2. Agency Address:		3. City/State/ZIP		4. Agency Code:	
5. Form Prepared By:		6. Title:		7. Telephone:		8. Email Address:	
Form Instructions: This form must be <u>typed</u> or <u>printed in ink</u> and be signed by the Chief Law Enforcement Officer. It is used to delete or modify <u>existing</u> registry information. To add new personnel, please use the Police Registry Entry Form / Certification of Initial Employment (DCJS 2214-A) . Mail completed forms to: NYS Division of Criminal Justice Services Office of Public Safety – Records Unit Alfred E. Smith State Office Building 80 South Swan St., 3rd Floor Albany, NY 12210							
9. Transaction Code		Enter "D" to delete an officer no longer appointed, "M" to modify the information of existing personnel. Circle the information to be modified.					
11. Social Security Number		Enter the officer's Social Security Number. The identifier is not mandatory; however the accuracy of training records cannot be assured without it.					
14. Change Date		Enter the effective date of the deletion or modification.					
15. Work Status		Enter "F" Full-time or "P" Part-time.					
16. Rank or Title		Enter the agency rank and/or title.					
9. Trans-action Code		10. Last Name, First Name, MI		11. Social Security Number*		12. Date of Birth mm/dd/yy	
						13. Sex M/F	14. Change Date
							15. Work Status P/F
							16. Rank or Title
I am the chief law enforcement officer responsible for appointing the persons named as police officers of the above named law enforcement agency. I understand that I am responsible to report employment transactions, pursuant to §845 of the Executive Law. I understand I am responsible to provide each police officer the required training, pursuant to §209-q of the General Municipal Law. I understand the information contained in this document is part of a written statement that will be presented to the Division of Criminal Justice Services for filing, and I certify that it is true to the best of my knowledge and belief.							
17. Chief Law Enforcement Officer Name - Printed				18. Chief Law Enforcement Officer Signature		19. Date	

***Pursuant to the New York State Personal Privacy Protection Law, DCJS is authorized to collect personal identifying information as part of a public safety agency record. Personal identifying information on this form shall not be revealed, released, transferred, disseminated or otherwise communicated orally, in writing, or by electronic means other than to the registrant. Disclosure of personal identifying information is voluntary. Refusal to provide personal identifying information shall not result in the denial of any right, benefit, or privilege.**

New York State Division of Criminal Justice Services
PEACE OFFICER REGISTRY ENTRY FORM - CERTIFICATION OF INITIAL EMPLOYMENT
(Executive Law § 845)

THIS FORM IS USED TO INITIALLY REGISTER A PEACE OFFICER WITH THE DIVISION OF CRIMINAL JUSTICE SERVICES. **USE THIS FORM FOR ALL INITIAL APPOINTMENTS AND TRANSFERS.** FORMS PRESENTED FOR FILING MUST CONTAIN ORIGINAL SIGNATURES. ALTHOUGH THE BLANK FORM MAY BE DUPLICATED, PHOTOCOPIES OF COMPLETED FORMS, OR FORMS WITH PHOTOCOPIED SIGNATURES WILL NOT BE ACCEPTED.

Pursuant to Executive Law §845, peace officer employers are required to register peace officers with the Division of Criminal Justice Services (DCJS). DCJS uses the peace officer registry to determine an individual's eligibility to receive a peace officer training certificate, and for other lawful purposes. DCJS reserves the right to require further documentation as necessary to properly classify a registrant. The information provided may be added to the registry and made available pursuant to law.

SECTION I: REGISTRANT INFORMATION

This section must be completed by the peace officer registrant. Only individuals appointed to positions defined in Criminal Procedure Law §2.10 or §2.16 are eligible for registration.

Type or print legibly, the registrant's last name, first name, middle initial, date of birth, and Social Security Number. Enter the complete home mailing address, home street address if different, and county of home residence. Temporary addresses are not acceptable. If the registrant is temporarily living away from home (e.g. enrolled at a college or university, on military assignment, etc.) **DO NOT** list the temporary address. Enter the registrant's city/state/country of birth (if other than U.S.). Registrants not born in the United States **MUST** include a certified copy of one of the following: (1) naturalization papers; (2) Department of State Birth certificate; or (3) currently valid United States Passport. Carefully read the certification. Sign and date in the area provided. With the exception of Social Security Number, the information in Section I is required. Incomplete submissions will not be processed.

SECTION II: AGENCY INFORMATION

Unless a written agreement is on file with DCJS, this section must be completed by the Chief Law Enforcement Officer (Chief, Sheriff, Director) of the appointing authority. In the case of municipalities with no designated Chief Law Enforcement Officer, the Town Supervisor or Village Mayor must be the signatory. The Executive Law mandates that all peace officers must be registered with the Division of Criminal Justice Services. The information in Section II identifies the law enforcement agency with which the registrant is a peace officer. Please refer to the Public Officers Law §3-b for eligibility and residency requirements.

Type or print legibly, the chief law enforcement officer's last name, first name and title. Enter the agency name, telephone number (including area code), and agency address. Enter the CPL 2.10 subdivision number, CPL subdivision title and weapons indicator for appointment of the person named in Section I. Indicate whether the appointment is full-time or part-time, whether background and residency checks were conducted, and if fingerprints were submitted to DCJS. Carefully read the certification. Sign and date in the area provided. The information in Section II is required. Incomplete submissions will not be processed. When signing this section, the CEO is verifying their responsibility to provide the registrant with the requisite training pursuant to CPL §2.30.

SECTION III: CIVIL SERVICE INFORMATION (FOR MUNICIPAL AND STATE EMPLOYERS ONLY)

This section must be completed for all registrants employed by a municipality or state agency, both full and part time, by the appropriate civil service commission officer. Civil Service Law mandates that the appointment of officers must meet certain requirements. The information in Section III describes the registrant's appointment.

If the registrant is employed by a private entity (i.e., the SPCA, or a Private College) it is **not** necessary to complete this section.

New York State Division of Criminal Justice Services
PEACE OFFICER REGISTRY ENTRY FORM - CERTIFICATION OF INITIAL EMPLOYMENT
(Executive Law § 845)

Type or print legibly, the civil service commission officer's last name, first name, middle initial and title. Enter the name, telephone number (including area code) and address of the civil service commission office. Enter the job title and civil service classification of the person named in Section I. This should be the specific title/classification to which the registrant was appointed and that appears on the agency payroll. Carefully read the certification. Sign and date in the area provided. The information in Section III is required. Incomplete submissions will not be processed.

SECTION IV: OATH OF OFFICE

This section must be completed by the appropriate registrar/recorder of oaths of office. Pursuant to Public Officers' Law §10 every peace officer that is a public officer must take and file an oath of office. The following persons are eligible to administer an oath of office:

- A judge of the court of appeals
- The Attorney General
- Any officer authorized to take the acknowledgment of the execution of a deed of real property
- An officer in whose office the oath is required to be filed or their duly designated assistant such as a City, Town, or Village Clerk (Municipal appointees) or the Fire Chief (Fire Police) or their designee.
- A presiding officer or clerk of a body of officers who has taken an oath of office (SPCA/SPCC/Private Entities)
- An oath of office may be administered to any state or local officer who is a member of the armed forces of the United States by any commissioned officer, in active service, of the armed forces of the United States

The Information in Section IV indicates the date the oath was taken by the registrant, the place of filing, and title of the office. Type or print legibly, the registrar/recording officer's last name, first name, middle initial and title. Enter the name, telephone number (including area code) and address of the registrar's / recorder's office. Carefully read the certification. Sign and date in the area provided. This section should be signed and dated once the officer named in Section I completes the oath of office for the agency named in Section I I and is the date recorded by DCJS as the appointment date of the officer. The information in Section IV is required. Incomplete submissions will not be processed.

MAILING INSTRUCTIONS

Mail completed forms to:

NYS Division of Criminal Justice Services
Alfred E. Smith State Office Building
Office of Public Safety – Records Unit
80 South Swan St., 3rd Floor
Albany, NY 12210-8002

QUESTIONS

If you have any questions regarding this form, call (518) 485-1092 for assistance.

New York State Division of Criminal Justice Services
PEACE OFFICER REGISTRY ENTRY FORM - CERTIFICATION OF INITIAL EMPLOYMENT
 (Executive Law § 845)

SECTION I – REGISTRANT INFORMATION (To be completed by the registrant)

Last Name	First Name	MI	Date of Birth	Gender M F	Social Security Number*
Home Residence Mailing Address		City, State, Zip		County of Home Residence	
Home Residence Street Address (if Different)		City, State, Zip		City, State, Country of birth (if other than U.S.)	
<i>I am the person named above. I understand that the information in Section I is part of a written statement that will be presented to the Division of Criminal Justice Services for filing, and I certify that it is true to the best of my knowledge and belief.</i>					
Signature					Date

*Pursuant to the New York State Personal Privacy Protection Law, DCJS is authorized to collect personal identifying information as part of a public safety agency record. Personal identifying information on this form shall not be revealed, released, transferred, disseminated or otherwise communicated orally, in writing, or by electronic means other than to the registrant. Disclosure of personal identifying information is voluntary. Refusal to provide personal identifying information shall not result in the denial of any right, benefit, or privilege.

SECTION II – AGENCY INFORMATION (To be completed by the chief law enforcement officer)

Last Name	First Name	MI	Title of Person Signing Section II
Name of Law Enforcement Agency			Telephone
Address		City, State, ZIP	
CPL §2.10 Subdivision	CPL Title/Position of Registrant	Weapons Indicator (Check/Circle All That Apply) NONE FIREARMS ASR BATON	
Type of Appointment Full-time Part-time	Background Check Conducted Yes No	Residency Verified Yes No	Fingerprints submitted to DCJS Yes No
<i>I am the chief law enforcement officer responsible for appointing the person named in Section I as a peace officer of the above named law enforcement agency. I understand that the information in Section II is part of a written statement that will be presented to the Division of Criminal Justice Services for filing, and I certify that it is true to the best of my knowledge and belief. I understand I am responsible for providing the registrant with the requisite training pursuant to CPL §2.30.</i>			
Signature			Date

SECTION III – CIVIL SERVICE INFORMATION (To be completed by the civil service officer for municipal and state registrants)

Last Name	First Name	MI	Title of Person Signing Section III
Name of Civil Service or Personnel Agency			Telephone
Address		City, State, ZIP	
Title and Civil Service Classification of the Registrant			
<i>I am the civil service officer responsible for certifying the appointment of individuals appearing on the payroll of the law enforcement agency named in Section II. I understand that the information in Section III is part of a written statement that will be presented to the Division of Criminal Justice Services for filing, and I certify that it is true to the best of my knowledge and belief.</i>			
Signature			Date

SECTION IV – OATH OF OFFICE (Public Officers Only - To be completed by the registrar responsible for recording oaths of office)

Last Name	First Name	MI	Title of Person Signing Section IV
Name of Recording Office			Telephone
Address		City, State, ZIP	
<i>I am the officer responsible for recording the oaths of office of individuals appointed as peace officers of the law enforcement agency named in Section II. The person named in Section I has filed an oath of office as a peace officer, pursuant to an appointment received from the person named in Section II. I understand that the information in Section IV is part of a written statement that will be presented to the Division of Criminal Justice Services for filing, and I certify that it is true to the best of my knowledge and belief.</i>			
Signature			Date Oath Administered

New York State Division of Criminal Justice Services
PEACE OFFICER REGISTRY UPDATE FORM
(Executive Law § 845-a)

Page of Pages

1. Agency Name:		2. Agency Address:		3. City/State/ZIP		4. Agency Code:					
5. Form Prepared By:		6. Title:		7. Telephone:		8. Email Address:					
Form Instructions: This form must be <u>typed</u> or <u>printed in ink</u> and be signed by the Chief Law Enforcement Executive or Employer. It is used to delete or modify <u>existing</u> registry information. To add new personnel, please use the Peace Officer Registry Entry Form – Certification of Initial Employment . Mail completed forms to: NYS Division of Criminal Justice Services Office of Public Safety – Records Unit Alfred E. Smith State Office Building 80 South Swan St. – 3rd Floor Albany, NY 12210											
9. Transaction Code		Enter "D" to delete an officer no longer appointed, "M" to modify the information of existing personnel. Circle the information to be modified.									
11. Social Security Number		Enter the officers Social Security Number. The identifier is not mandatory, however the accuracy of training records cannot be assured without it.									
14. Change Date		Enter the effective date of the deletion or modification.									
15. Work Status		Enter "F" Full-time or "P" Part-time.									
17. Weapon Indicator		Check the appropriate box(es) for the weapons the officer will have access to during the course of their official duties (select all that apply)									
9. Trans- action Code	10. Last Name, First Name, MI	11. Social Security Number*	12. Date of Birth mm/dd/yy	13. Sex M/F	14. Change Date mm/dd/yy	15. Work Status P/F	16. Rank or Title	17. Weapon Indicator (Select all that apply)			
								None	Firearm	ASR	Baton
<i>I am the chief law enforcement executive, or employer, responsible for the persons named as peace officers of the above named law enforcement agency. I understand that I am responsible to report employment transactions, pursuant to §845-a of the Executive law. I understand I am responsible to provide each peace officer the required training, pursuant to §2.30 of the Criminal Procedure Law. I understand the information contained in this document is part of a written statement that will be presented to the Division of Criminal Justice Services for filing, and I certify that it is true to the best of my knowledge and belief.</i>											
17. Chief Law Enforcement Officer (or Employer) Name- Printed		19. Chief Law Enforcement Officer (or Employer) Signature					19. Date				

*Pursuant to the New York State Personal Privacy Protection Law, DCJS is authorized to collect personal identifying information as part of a public safety agency record. Personal identifying information on this form shall not be revealed, released, transferred, disseminated or otherwise communicated orally, in writing, or by electronic means other than to the registrant. Disclosure of personal identifying information is voluntary. Refusal to provide personal identifying information shall not result in the denial of any right, benefit, or privilege.

New York State Division of Criminal Justice Services
CURRICULUM CONTENT FORM
(9)NYCRR 6020, 6021, 6022, 6025

THIS FORM IS USED TO FILE ALL COURSES WITH THE DIVISION OF CRIMINAL JUSTICE SERVICES (DCJS) FOR BOTH MUNICIPAL POLICE TRAINING COUNCIL (MPTC) APPROVED AND/OR DCJS APPROVED COURSES. FORMS PRESENTED FOR FILING MUST CONTAIN ORIGINAL SIGNATURES. ALTHOUGH THE BLANK FORM MAY BE DUPLICATED, PHOTOCOPIES OF COMPLETED FORMS, OR FORMS WITH PHOTOCOPIED SIGNATURES WILL NOT BE ACCEPTED.

Pursuant to *Title 9 of the Official Compilation of Codes, Rules and Regulations of the State of New York, Parts 6020.4(a), 6021.4(a), 6022.4(a)*, no later than 45 days prior to the commencement of a course, the course director shall file a copy of the proposed curriculum with the commissioner. This curriculum shall be in a form prescribed by the commissioner and shall include the course location and sponsor, chronological listing of topics and hours allotted and the names and certifications of instructors.

Completing the top of the form:

1. **Course Title:** Enter the course title. If the curriculum has been approved by the Municipal Police Training Council, enter the MPTC approved course title. Documentation that fails to utilize the MPTC approved course title will be rejected. For example "RADAR Operator Course."
2. **Course Sponsor:** Enter the name of the agency or department administering the course. Only recognized law enforcement agencies are eligible to provide peace and/or police training courses. For example: "Zone Five Law Enforcement Training Center."
3. **School Location:** Enter the address where training will be conducted. For example: Onondaga Community College, Syracuse, NY.
4. **Course Date(s):** Enter the date the course begins and ends. For example: April 1 - 4, 2004.
5. **Course Director:** Enter the school director's name. This is the person responsible for administering the course and all required paperwork. This person may be an instructor or academy director. All correspondence will be directed to this person.

Completing the lower portion of the form:

1. **Date:** Enter the date for which the topic/module will be presented. For example: 04/01/04.
2. **Instructional Start Time:** Enter the time at which the topic/module will begin. For example: 08:00.
3. **Hours Assigned:** Enter the number of hours assigned to the topic/module. For example: 2.
4. **MPTC Course Title:** Enter the MPTC approved title for the topic/module according to the instructor guide. For example: "RADAR Principles."
5. **Academy Course Title:** This field is optional, but you may enter the course title utilized by the local training provider.
6. **Instructor*:** Enter the first name, last name, and agency name of the instructor. For example:

Lt. John Smith
Police Department
7. **OPS Status:** Enter the instructor status, or certifications, of the named instructor. For example: RL (Radar Lidar) or GT (General Topics).
8. **Expiration Date:** Enter the date the instructor's certification expires. For example: 12/31/08.

* If an instructor is used multiple times throughout a course, a last name is sufficient so long as all required information is supplied under the first entry.

Pursuant to NYS regulations, this form must be submitted 45 days prior to the proposed start date of the course.

COURSE TITLE:

**SCHOOL
SPONSOR:
SCHOOL
LOCATION:**

SCHOOL DATES:

SCHOOL DIRECTOR:

DATE	INSTRUCTIONAL START TIME	HOURS ASSIGNED	MPTC COURSE TITLES (REQUIRED)	ACADEMY COURSE TITLE (OPTIONAL)	INSTRUCTOR NAME AND DEPARTMENT	INSTRUCTOR CERTIFICATIONS	EXPIRATION DATE

To School Director: TYPE the name, social security number, date of birth, sex, employing agency, rank, and status code of each student. Have each student verify the spelling and accuracy of his/her individual information. Complete all sections as indicated with the exception of those designated for completion and OPS USE. Indicate if an employing agency is a town (T/O), village (V/O), city C/O), or county (CO/O) department. Do not use any abbreviations. Return one copy of this roster to the OPS Training Unit at the address listed below within 5 working days after the starting date of any MPTC course exceeding 35 hours. Retain one copy of this roster in your school file. At the conclusion of the course, note the performance of each student in the section entitled completion (S=satisfactory, U=unsatisfactory). Sign, date, and forward to the Training Unit within 5 working days.

NAME OF SCHOOL/ACADEMY:
ADDRESS OF SCHOOL/ACADEMY:
SCHOOL DIRECTOR:
COURSE NAME:
DATE(S) OF COURSE:

FOR OPS USE

IN

OUT

SCHOOL ID #

COURSE CODE

HOURS

Name of Trainee (Last, First, MI)	SS#	DOB	Sex	Employing Agency	Status*	Rank	Appt. Date	S/U	Code	Current Permit Exp. Date	Permit #	New Permit Exp. Date
1.												
2.												
3.												
4.												
5.												
6.												
7.												
8.												
9.												
10.												

Status Code: POL/F=Police Officer Full Time PEA/F=Peace Officer Full Time CIV=Civilian
POL/P=Police Officer Part Time PEA/P=Peace Officer Part Time

NYS Division of Criminal Justice Services
Office of Public Safety
Alfred E. Smith Office Building
80 South Swan Street, 3rd Floor
Albany, NY 12210-8002
518 457-2667

** Complete this section at the conclusion of a course if student performance is known.
*** This date should reflect the date appointed to the listed employing agency. For the Course in Police Supervision, the date of promotion.
I hereby certify that the above named students have, where indicated, successfully completed all aspects of this course and have not missed a greater number of hours than that permitted by rule or statute. I further certify that the curriculum for this course has not been substantially altered in either content or duration from that which was approved. I hereby attach a description of alterations made, if any, to the approved curriculum. I affirm under penalty of perjury that the statements made on this form, including all attachments, are true.

State of New York Division of Criminal Justice Services
NOTIFICATION OF TERMINATION / RESIGNATION FROM TRAINING
(9 NYCRR 6020.5(c) , 9 NYCRR 6021.5(d))

THIS FORM IS USED TO ADVISE THE NEW YORK STATE DIVISION OF CRIMINAL JUSTICE SERVICES OF THE TERMINATION OR RESIGNATION OF A RECRUIT FROM POLICE BASIC TRAINING OR A FIRST-LINE SUPERVISOR FROM THE COURSE IN POLICE SUPERVISION. FORMS PRESENTED FOR FILING MUST CONTAIN ORIGINAL SIGNATURES. ALTHOUGH THE BLANK FORM MAY BE DUPLICATED, PHOTOCOPIES OF COMPLETED FORMS, OR FORMS WITH PHOTOCOPIED SIGNATURES WILL NOT BE ACCEPTED.

SECTION - TRAINING COURSE (Check appropriate box)

☐ Basic Course for Police Officers ☐ Specialized Investigator Police Training Course ☐ Course in Police Supervision

SECTION II – RECRUIT INFORMATION (To be completed by the course director)

Last Name		First Name		MI
Social Security Number*	Date of Birth		Gender	
Employer				

*Pursuant to the New York State Personal Privacy Protection Law, DCJS is authorized to collect personal identifying information as part of a public safety agency record. Personal identifying information on this form shall not be revealed, released, transferred, disseminated or otherwise communicated orally, in writing, or by electronic means other than to the registrant. Disclosure of personal identifying information is voluntary. Refusal to provide personal identifying information shall not result in the denial of any right, benefit, or privilege.

SECTION III – TRAINING PROVIDER (To be completed by the course director)

Name of Training Academy		Telephone	
Address	City, State, ZIP		
Course Director Name		Dates of Training to	
Course Director Signature			Date

SECTION IV – REASON FOR TERMINATION / RESIGNATION (Brief narrative description of factors surrounding removal)

If you require additional space, attach an additional sheet and follow the same format. Supporting documentation may be attached.

Mailing Instructions

Mail completed forms to:

NYS Division of Criminal Justice Services
Office of Public Safety – Records Unit
Alfred E. Smith State Office Building
80 South Swan St.
Albany, NY 12210

DCJS USE ONLY

Date Received:	Reviewed By:	Data Entry Date:

State of New York Division of Criminal Justice Services
PRE-EMPLOYMENT POLICE BASIC TRAINING PROGRAM – SCHOOL APPLICATION

THIS FORM IS USED TO APPLY FOR APPROVAL OF A PRE-EMPLOYMENT POLICE BASIC TRAINING PROGRAM TO BE PROVIDED JOINTLY BY A CRIMINAL JUSTICE PROGRAM OF AN ACCREDITED COLLEGE IN CONJUNCTION WITH A LOCAL LAW ENFORCEMENT ACADEMY. INFORMATION PROVIDED ON THE APPLICATION MUST BE **TYPED** OR **PRINTED CLEARLY** IN ORDER FOR IT TO BE PROCESSED. LACK OF ANY REQUIRED INFORMATION WILL **STOP** THE APPROVAL PROCESS. FORMS PRESENTED FOR FILING MUST CONTAIN ORIGINAL SIGNATURES. ALTHOUGH THE BLANK FORM MAY BE DUPLICATED, PHOTOCOPIES OF COMPLETED FORMS, OR FORMS WITH PHOTOCOPIED SIGNATURES WILL NOT BE ACCEPTED.

SECTION I - GENERAL INFORMATION

Pre-employment training shall be presented jointly by a municipality and an accredited college, junior college, or two-year college, that has an active criminal justice, or equivalent, program that has been registered and approved by the Department of Education, located within the State of New York.

Name of School

Enter the name of the school in the blocks provided. List the complete street address of the school (do not enter only a post office box) Email address, and county. Enter the Internet address, business telephone and facsimile numbers, including area code, at the school. A list of approved schools will be published on the DCJS web site.

College Information

PRINT CLEARLY or **TYPE** the required information in the spaces provided concerning the institution. Provide the institution mailing address, the telephone and facsimile numbers, including area code, and where the chief executive officer may be contacted during daytime business hours.

Municipality Information

PRINT CLEARLY or **TYPE** the required information in the spaces provided concerning the municipality (including law enforcement agencies, academies, police academies, or training centers sponsored by municipalities). Provide the institution mailing address, the telephone and facsimile numbers, including area code, and where the chief executive officer (police chief, sheriff, academy director) may be contacted during daytime business hours.

Director Information

Enter the director's name, mailing address, Email address, telephone and facsimile number, including area code, and where the director may be contacted during daytime business hours. Provide their social security number.

ALL CORRESPONDENCE WILL BE SENT TO THE DIRECTOR AT THE ADDRESS PROVIDED.

Alternate Director Information (Optional)

Enter the alternate director's name. This staff member is authorized to act on behalf of the School director in their absence.

SECTION II - DESCRIPTION OF FACILITY

Facilities

Briefly describe the classroom, emergency vehicle driving, and physical fitness facilities on the lines provided. Certify that the institution meets the standards established by the Commissioner of Education for instructional resources set forth in §52.2 of Title 8, Chapter II of the Regulations of the Commissioner.

If you are seeking approval for more than one location, the information in Section II must be provided for each proposed training site. This information must include the name of the school, training site, address, county, telephone number and description of facility. Duplicate Section II as needed.

SECTION III - CURRICULUM AND CERTIFIED INSTRUCTORS

Curriculum

Certify that the topics, instructional hours, instructional objectives, and curriculum outline meets or exceeds the standard established pursuant to the rules and regulations codified in Title 9 of the *Official Compilation of Codes, Rules and Regulations of the State of New York* Part 6020 and Part 6026.

State of New York Division of Criminal Justice Services
PRE-EMPLOYMENT POLICE BASIC TRAINING PROGRAM – SCHOOL APPLICATION

Instructors

Certify that each instructor in pre-employment training is certified or approved pursuant to the rules and regulations codified in Title 9 of the *Official Compilation of Codes, Rules and Regulations of the State of New York* Part 6023 and Part 6024. **Certain units of training require that instructors have additional topical experience and/or instructor training.**

Certified instructor(s) must possess a current general topics certificate issued by the State of New York Municipal Police Training Council (MPTC). Schools must maintain a file copy of each certificate.

Approved instructor(s) must possess an instructor approval letter issued by the Division of Criminal Justice Services that details the specific topic(s) the instructor is permitted to teach. Schools must maintain a file copy of each letter.

Complete and submit the Curriculum Content Form with the application.

SECTION IV - SCHOOL POLICY

Policy

Certify that the school has policy that has been established for the administration of the school pursuant to Title 9 of the *Official Compilation of Codes, Rules and Regulations of the State of New York* Part 6023 and Part 6026. Submit a copy of the policy with the application.

SECTION V - ATTESTATION

Applicant Signatures

This section must be signed and sworn to by the chief executive officer of both the college, two-year college, or junior college AND the municipality (including law enforcement agencies, academies, police academies, or training centers sponsored by municipalities) before a notary public.

Mailing Instructions

Processing will be facilitated if **all** documentation is submitted as **one** package. **Include** with the application **all** additional sheets for descriptions of training facilities and range locations.

Mail the completed application to:

NYS Division of Criminal Justice Service
Office of Public Safety - Course Approval
Alfred E. Smith State Office Building
80 South Swan Street, 3rd Floor
Albany, NY 12210-8002

After review and approval of this application by DCJS staff, an approval letter will be issued. Approvals will be valid for a period of two years.

If you have any questions regarding the application, call (518) 485-7619 (Select - police or peace officer training course approval) for assistance.

Information provided on the application must be **typed** or **printed clearly** in order for it to be processed. Lack of any required information will **stop** the school approval process.

State of New York Division of Criminal Justice Services
PRE-EMPLOYMENT POLICE BASIC TRAINING PROGRAM – SCHOOL APPLICATION

SECTION I - GENERAL INFORMATION

School Information

☐ Original Application ☐ Renewal Application		
School Name		MPTC Training Zone
Address	City, State, Zip	County
Email Address	Telephone Number (area code first)	Facsimile Number (area code first)
Internet Web Address		

College Information

Institution Name	CEO/Title	
Address	City, State, Zip	County
Email Address	Telephone Number (area code first)	Facsimile Number (area code first)
Name of Accreditation Body	Current Dates of Accreditation	Date of Dept. of Ed CJ Program Approval

Municipality Information

Municipality Name	CEO/Title	
Address	City, State, Zip	County
Email Address	Telephone Number (area code first)	Facsimile Number (area code first)

Director Information

Director Name	Employer	
Address	City, State, Zip	Address
Email Address	Telephone Number (area code first)	Email Address

Alternate Director Information (Optional)

Director Name	Employer	
Address	City, State, Zip	County
Email Address	Telephone Number (area code first)	Facsimile Number (area code first)

State of New York Division of Criminal Justice Services
PRE-EMPLOYMENT POLICE BASIC TRAINING PROGRAM – SCHOOL APPLICATION

SECTION II - DESCRIPTION OF FACILITY

Classroom Facilities (check one)

☐	Briefly describe the classroom(s) including seating accommodations, restroom availability, audio-visual display equipment, and heating and ventilation:
☐	or the signatories certify that the institution meets the standards established by the Commissioner of Education for instructional resources set forth in § 52.2 of Title 8, Chapter II of the Regulations of the Commissioner

Emergency Vehicle Driver Training Facilities

Briefly describe the emergency vehicle driver training facilities:

Physical Fitness Facilities (check one)

☐	Briefly describe the physical fitness facilities:
☐	or the signatories certify that the institution meets the standards established by the Commissioner of Education for instructional resources set forth in § 52.2 of Title 8, Chapter II of the Regulations of the Commissioner

SECTION III - CURRICULUM and CERTIFIED INSTRUCTORS

Curriculum

Execution of this application certifies that the topics, instructional hours, instructional objectives, and curriculum outline meet or exceed the standards established pursuant to the rules and regulations codified in Title 9 of the *Official Compilation of Codes, Rules and Regulations of the State of New York* Part 6020 and Part 6026. Complete and submit the Curriculum Content Form provided.

Instructors

Execution of this application certifies that each instructor used in pre-employment training is certified or approved pursuant to the rules and regulations codified in Title 9 of the *Official Compilation of Codes, Rules and Regulations of the State of New York* Part 6023 and Part 6024.

SECTION IV - SCHOOL POLICY

Policy

Execution of this application certifies that the school has policies established pursuant to the rules and regulations codified in Title 9 of the *Official Compilation of Codes, Rules and Regulations of the State of New York* Part 6026. Submit the a copy of the policy with the application.

State of New York Division of Criminal Justice Services
PRE-EMPLOYMENT POLICE BASIC TRAINING PROGRAM - SCHOOL APPLICATION

SECTION V – ATTESTATION

College Chief Executive Officer Attestation: This affidavit must be signed and sworn to by the applicant before a Notary Public. I hereby attest that the information in this application is true to the best of my knowledge and belief. I understand that any omission or inaccuracy may be deemed sufficient reason to deny certification. I understand the Division of Criminal Justice Services may ask for additional information or documentation.

Notary Stamp

Applicant Signature: _____

Sworn and subscribed to before me this _____ day of _____, 20____

Notary Signature: _____

Execution of this application by the signatories certifies compliance with the policy, procedures, rules, and regulations established by the Division of Criminal Justice Services and the Municipal Police Training Council.

Municipality Executive Officer (sheriff, police chief, or academy director) Attestation: This affidavit must be signed and sworn to by the applicant before a Notary Public. I hereby attest that the information in this application is true to the best of my knowledge and belief. I understand that any omission or inaccuracy may be deemed sufficient reason to deny certification. I understand the Division of Criminal Justice Services may ask for additional information or documentation.

Notary Stamp

Applicant Signature: _____

Sworn and subscribed to before me this _____ day of _____, 20____

Notary Signature: _____

Execution of this application by the signatories certifies compliance with the policy, procedures, rules, and regulations established by the Division of Criminal Justice Services and the Municipal Police Training Council.

DCJS ONLY

☐ Curriculum Meets or Exceeds Regulation ☐ Instructors Compliant ☐ Policy Compliant ☐ Other: _____

Approved by:

Date

Approval Letter Date:

New York State Division of Criminal Justice Services
PRE-EMPLOYMENT POLICE BASIC TRAINING PROGRAM CURRICULUM CONTENT FORM
 (9 NYCRR 6026), Updated 2006, 2008

School Name	Director's Name	Date of Submission

Basic Course for Police Officers Part/Module Name	Required Hours	Actual Hours	Credit Course Name (If applicable)	Instructor Name / SSN	Instructor Status Certified or Approved	Instructor Certification Expiration Date	DCJS USE
Part 1 – Administration of Justice							
1-A. Introduction to Criminal Justice							
1-B. Jurisdictions and Responsibilities of Law Enforcement							
1-C. Adjudicatory Process and Court Structure Civil & Criminal							
Total	4						
Part 2 – Introduction to Law Enforcement							
2-A. Constitutional Law	2						
2-B. Discretionary Powers	2						
2-C. Ethical Awareness	12						
2-D. Physical Fitness and Wellness	65						
Total	81						
Part 3- Laws of New York State							
3-A. New York State Penal Law Offenses	16						
3-B. Justification - Use of Physical Force & Deadly Physical Force	7						
3-C. New York State Criminal Procedure Law	21						
Standards of Proof							
Laws of Arrest							

New York State Division of Criminal Justice Services
PRE-EMPLOYMENT POLICE BASIC TRAINING PROGRAM CURRICULUM CONTENT FORM
 (9 NYCRR 6026), Updated 2006, 2008

Basic Course for Police Officers Part/Module Name	Required Hours	Actual Hours	Credit Course Name (If applicable)	Instructor Name / SSN	Instructor Status Certified or Approved	Instructor Certification Expiration Date	DCJS USE
Part 3 – Laws of New York State (continued)							
Search and Seizure							
Stop, Question, and Frisk							
Interview and Interrogation							
Accusatory Instruments							
Appearance Tickets							
Evidence Concepts							
Eyewitness ID							
3-D. New York State Juvenile Law and Procedures	5						
3-E. Civil Liability and Risk Management	2						
3-F. Ancillary New York State Statutes	2						
3-G. New York State Vehicle and Traffic Law	5						
Total	58						
Part 4 – Law Enforcement Skills							
4-A. Field Note-Taking	2						
4-B. Report Writing	7						
4-C. Communications	4						
4-D. Observation and Patrol	4						

New York State Division of Criminal Justice Services
PRE-EMPLOYMENT POLICE BASIC TRAINING PROGRAM CURRICULUM CONTENT FORM
 (9 NYCRR 6026), Updated 2006, 2008

Basic Course for Police Officers Part/Module Name	Required Hours	Actual Hours	Credit Course Name (If applicable)	Instructor Name / SSN	Instructor Status Certified or Approved	Instructor Certification Expiration Date	DCJS USE
Part 4 – Law Enforcement Skills (continued)							
4-E. Case Preparation and Demeanor in Official Proceedings	7						
4-F. Mental Illness	14						
4-G. Crimes in Progress	4						
4-H. Arrest Processing	5						
4-I. Professional Traffic Stops	5						
4-J. Interpersonal Skills - Arrest Techniques	40						
Communication/Interpersonal Skills							
Defensive Tactics							
Aerosol Devices							
Impact Devices (training batons only)							
Crowd and Riot Control Formations							
Rapid Deployment and Active Shooter							
4-K. Emergency Medical Services	40						
4-L. Emergency Vehicle Operation and Control	21						
4-M. Firearms Training	40						
4-N. Supervised Field Training Review and Orientation	160						

New York State Division of Criminal Justice Services
PRE-EMPLOYMENT POLICE BASIC TRAINING PROGRAM CURRICULUM CONTENT FORM
 (9 NYCRR 6026), Updated 2006, 2008

Basic Course for Police Officers Part/Module Name	Required Hours	Actual Hours	Credit Course Name (if applicable)	Instructor Name / SSN	Instructor Status Certified or Approved	Instructor Certification Expiration Date	DCJS USE
Part 4 – Law Enforcement Skills (continued)							
4-O. Traffic Direction and Control	2						
4-P. Traffic Enforcement	4						
4-Q. DWI Detection and Standardized Field Sobriety Testing	21						
4-R. Physical Evidence	12						
4-S. Off Duty and Plain Clothes Police Encounters	2						
Total	194						
Part 5 – Community Interaction							
5-A. Intoxication	2						
5-B. Community Resources - Victim/Witness Services	3						
5-C. Crime Prevention and Crime Against the Elderly	4						
5-D. Cultural Diversity/Bias Related Incidents and Sexual Harassment	5						
5-E. Persons with Disabilities	2						
5-F. Community Oriented Policing and Problem Solving - Media Relations	2						
Total	18						

New York State Division of Criminal Justice Services
PRE-EMPLOYMENT POLICE BASIC TRAINING PROGRAM CURRICULUM CONTENT FORM
 (9 NYCRR 6026), Updated 2006, 2008

Basic Course for Police Officers Part/Module Name	Required Hours	Actual Hours	Credit Course Name (if applicable)	Instructor Name / SSN	Instructor Status Certified or Approved	Instructor Certification Expiration Date	DCJS USE
Part 6- Mass Casualties and Major Events							
6-A. Standardized Response Plans for Unusual Events	8						
~~6-B. Counter Terrorism~~	8						
Weapons of Mass Destruction							
Bombs and Bomb Threats							
Commercial Vehicle and Transportation Enforcement							
Document/Identification Fraud							
6-C. The Nature and Control of Civil Disorder	2						
Total	10						
Part 7 - Investigations							
7-A. Domestic Violence	14						
7-B. Organized Crime Familiarization/Enterprise Corruption	2						
7-C. Preliminary Investigation and Information Development	2						
7-D. Interviewing Techniques	5						
7-E. Common Criminal Investigation Techniques	10						
Larceny							
Auto Theft							
Burglary							

New York State Division of Criminal Justice Services
PRE-EMPLOYMENT POLICE BASIC TRAINING PROGRAM CURRICULUM CONTENT FORM
 (9 NYCRR 6026), Updated 2006, 2008

Basic Course for Police Officers Part/Module Name	Required Hours	Actual Hours	Credit Course Name (if applicable)	Instructor Name / SSN	Instructor Status Certified or Approved	Instructor Certification Expiration Date	DCJS USE
Part 7 – Investigations (continued)							
Robbery							
Arson							
Electronic Media							
7-F. Basic Crash Management and Reporting	14						
7-G. Injury and Death Cases	3						
7-H. Sex Crimes	2						
7-I. Narcotics and Dangerous Drugs	3						
7-J. Missing and Abducted Children - Missing Adult Cases	3						
7-K. Animal Abuse Cases	2						
7-L. Contemporary Police Problems	4						
7-M. Human Trafficking	2						
Total	66						
Total Program Hours	431						

2006 Added Animal Abuse unit (2 hours)
 2008 Added Off Duty and Plain Clothes Police Encounters Unit (2 hours) and Human Trafficking Unit (2 hours)

PRE-EMPLOYMENT POLICE BASIC TRAINING PROGRAM – STUDENT ADVISORY NOTICE

THIS FORM IS USED TO ENSURE STUDENTS ATTENDING A PRE-EMPLOYMENT POLICE BASIC TRAINING PROGRAM HAVE BEEN ADVISED OF THE PROGRAM REQUIREMENTS AND RULES AND REGULATIONS GOVERNING TRAINING AND APPOINTMENT AS A POLICE OFFICER. FORMS PRESENTED FOR FILING MUST CONTAIN ORIGINAL SIGNATURES. ALTHOUGH THE BLANK FORM MAY BE DUPLICATED, PHOTOCOPIES OF COMPLETED FORMS, OR FORMS WITH PHOTOCOPIED SIGNATURES WILL NOT BE ACCEPTED.

Students in the Pre-Employment Police Basic Training Course must be advised of several conditions of this training program that will affect them during and after attending the program. Schools are required to advise the student of these conditions by the policy established for this program by Division of Criminal Justice Services.

1. Completion of this program is **not a guarantee of employment** as a police officer.
2. To complete this pre-employment training program, a student must participate in physical fitness training and successfully complete a physical fitness examination.
3. To complete this pre-employment training program, a student must comply with mandated New York State regulations that include: strict attendance requirements; maintaining a notebook; and passing written examination/s.
4. This is a two-phase program. The first phase is conducted pre-employment and **the second phase is conducted after appointment as a police officer**. Each individual phase of this training program must be completed as a single and cohesive unit. This means that students must complete the phase of the program at one institution. The following phase may be conducted at a separate institution.
5. Before being appointed as a police officer, a person must complete New York State Civil Service requirements and appointing agency hiring standards (including minimum and maximum age and residency requirements) by taking a written examination and scoring high enough on the eligibility list to be considered for appointment.
6. Before being appointed as a police officer, a person must take and successfully complete a physical fitness examination.
7. Before being appointed as a police officer, a person must submit to a medical examination, which may include drug screening.
8. Before being appointed as a police officer, a person may be required to submit to a psychological examination.
9. Before being appointed as a police officer, a person with criminal conviction or with a felony conviction may be disqualified from employment.
10. Before being appointed as a police officer, a person may be required to submit to a background investigation.
11. Upon appointment as a police officer, a person will be required to successfully complete additional training. Failure to complete this training will result in denial of certification by the New York State Municipal Police Training Council. This certification is required by § 209-q of the General Municipal Law for police officers to remain in their positions.
12. Pre-employment training will be valid for two years after completion of this program. If a person is not appointed before two years has elapsed, they will be required to attend a Police Refresher Course. After ten years from the date of completion records on the transcript, the training will no longer be valid (this is consistent with the provision of §209-q of the General Municipal Law pertaining to police officers).

ATTESTATION

Applicant Attestation: I hereby attest that I have read and understand the above policies regarding the Pre-Employment Police Basic Training Program. I understand that the information in this section is part of a written statement that will be presented to the Division of Criminal Justice Services for filing, and I certify that it is true to the best of my knowledge and belief.

Student Signature	Date
School Director Signature	Date

State of New York Division of Criminal Justice Services
REQUEST FOR TRAINING INFORMATION FORM

THIS FORM IS USED TO REQUEST TRAINING RECORDS INFORMATION FROM THE NEW YORK STATE DIVISION OF CRIMINAL JUSTICE SERVICES, OFFICE OF PUBLIC SAFETY (DCJS). ALL RECORDS WILL REFLECT TRAINING REPORTED TO DCJS AS OF THE DATE OF REQUEST. FORMS PRESENTED FOR FILING MUST CONTAIN ORIGINAL SIGNATURES. ALTHOUGH THE BLANK FORM MAY BE DUPLICATED, PHOTOCOPIES OF COMPLETED FORMS, OR FORMS WITH PHOTOCOPIED SIGNATURES WILL NOT BE ACCEPTED.

SECTION I - RECORDS REQUESTED

- | |
|---|
| ☐ Official Copy of Security Guard Program Training Records (Complete Section II Only) |
| ☐ Official Copy of Training Records (Complete Sections II & III) |
| ☐ Determination of the validity of my Basic Course for Police Officer / Peace Officer Certificate (Complete Sections II & III) |

SECTION II - APPLICANT INFORMATION (To be completed by the applicant)

Last Name	First Name	MI	Date of Birth	Social Security Number*
Mailing Address	City, State, Zip		Daytime Telephone #	
Email address				
Location of Basic Training			Date(s)	
Have you had an interruption in continuous police or peace officer service or a reassignment while employed as a police or peace officer since receiving your Basic Course For Police/Peace Officer certificate?			☐ Yes (describe below) ☐ No	
Signature			Date	

*Pursuant to the New York State Personal Privacy Protection Law, DCJS is authorized to collect personal identifying information as part of a public safety agency record. Personal identifying information on this form shall not be revealed, released, transferred, disseminated or otherwise communicated orally, in writing, or by electronic means other than to the registrant. Disclosure of personal identifying information is voluntary. Refusal to provide personal identifying information shall not result in the denial of any right, benefit, or privilege.

SECTION III - LAW ENFORCEMENT TRAINING (For law enforcement records only)

Name of Law Enforcement Agency Employed by During Training		Telephone
Address	City, State, ZIP	
Name of Training Academy	Dates of Basic Police Training to	
Have You Had An Interruption In Continuous Service Since Receiving Your Certificate? If so, please describe in Section III.		☐ Yes ☐ No

If you require additional space, attach an additional sheet and follow the same format.

Comments

Mailing Instructions

Mail completed forms to:

NYS Division of Criminal Justice Services
Alfred E. Smith State Office Building
Office of Public Safety – Records Unit
80 South Swan St., 3rd Floor
Albany, NY 12210

DCJS USE ONLY

Date Received:	Assigned To:	Reply Mailed:

New York State Division of Criminal Justice Services
WAIVER OF POLICE OFFICER TRAINING REQUIREMENT
(Executive Law §841)

THIS FORM IS USED BY PERSONS WHO HAVE RECEIVED PRIOR CERTIFICATION OF POLICE BASIC TRAINING, FROM THE NEW YORK STATE POLICE OR NEW YORK CITY POLICE DEPARTMENT OR WHILE FORMERLY EMPLOYED AS A PEACE OFFICER. FORMS PRESENTED FOR FILING MUST CONTAIN ORIGINAL SIGNATURES. ALTHOUGH THE BLANK FORM MAY BE DUPLICATED, PHOTOCOPIES OF COMPLETED FORMS, OR FORMS WITH PHOTOCOPIED SIGNATURES WILL NOT BE ACCEPTED.

Executive Law §841(3) authorizes the commissioner of the Division of Criminal Justice Services to certify police basic training, and to issue equivalency certificates to former State University of New York Public Safety Officers appointed prior to January 1, 1999, or to former peace officers who have completed a Basic Course for Police Officers approved by the Municipal Police Training Council for the purposes of satisfying the training requirements established by General Municipal Law (GML) §209-q. Certification is contingent upon demonstration of the completion of supervised field training, requisite job-related law enforcement experience as determined by the commissioner, and if deemed necessary, the successful completion of relevant police officer training courses pursuant to GML §209-q.

SECTION I: APPLICANT INFORMATION

This section must be completed by the chief executive officer of the applicant's current employer. Type or print legibly, the applicant's last name, first name, middle initial, date of birth, social security number, and gender. Enter the name of the current employer, the rank and/or title of the applicant, and the date of initial appointment. While the Social Security Number is not required, the accuracy of linking future training records with appointment information cannot be assured without it. Carefully read the certification. Sign and date in the area provided. With the exception of Social Security Number, the information in Section I is required. Incomplete submissions will not be processed.

SECTION II: PREVIOUS POLICE OR PEACE OFFICER EXPERIENCE

Type or print legibly, the agency name, telephone, complete mailing address, title or rank of the applicant, type of appointment (full or part-time), the date of appointment and the date of separation from service (if any). Repeat for each police employer. Incomplete submissions will not be processed.

The provisions of General Municipal Law §209-q regarding the validity of police officer basic training certification applies to newly appointed police officers, regardless of past employment. For example, a former NYPD or NYSP member who has been separated for more than four years and is then appointed as a police officer with a town police department must complete the Police Refresher Course within twelve months of appointment.

SECTION - III: POLICE BASIC TRAINING

Type or print legibly, the name, telephone, complete mailing address of the academy that provided the basic training course. Include the name of the course director and the dates of the course. Incomplete submissions will not be processed. **A photocopy of the certificate of completion or official transcript must be attached.**

MAILING INSTRUCTIONS:

Mail completed forms to:

NYS Division of Criminal Justice Services
Office of Public Safety – Records Unit
Alfred E. Smith State Office Building
80 South Swan St., 3rd Floor
Albany, NY 12210

QUESTIONS:

If you have any questions regarding this form, call (518) 485-1092 for assistance.

New York State Division of Criminal Justice Services
WAIVER OF POLICE OFFICER TRAINING REQUIREMENT
(Executive Law §841)

SECTION I – APPLICANT INFORMATION (To be completed by the chief law enforcement officer)

Applicant Last Name	Applicant First Name	MI	Date of Birth	Social Security Number*	Gender ☐ M ☐ F
New York Employer (applicant must be appointed to a police officer title in NYS)		Rank or Title		Date of Appointment	
<i>I hereby certify the above named individual has been appointed as a sworn police officer with this agency. I have determined that he/she has completed the basic training course while employed as a police officer in the United States of Territories thereof. Accordingly, I request that the Division of Criminal Justice Services review and evaluate the enclosed documentation for satisfaction of all or part of the basic training requirements for police officers as established by General Municipal Law section 209-q. I understand that the information in Section I is part of a written statement that will be presented to the Division of Criminal Justice Services for filing, and I certify that it is true to the best of my knowledge and belief.</i>					
Signature of Chief Executive Officer				Date	

*Pursuant to the New York State Personal Privacy Protection Law, DCJS is authorized to collect personal identifying information as part of a public safety agency record. Personal identifying information on this form shall not be revealed, released, transferred, disseminated or otherwise communicated orally, in writing, or by electronic means other than to the registrant. Disclosure of personal identifying information is voluntary. Refusal to provide personal identifying information shall not result in the denial of any right, benefit, or privilege.

SECTION II – PREVIOUS POLICE OFFICER EXPERIENCE

Identify previous police employment.			
Name of Previous Law Enforcement Employer			Telephone
Address		City, State, ZIP	
Rank or Position	Type of Appointment ☐ Full-time ☐ Part-time	Date of appointment	Date of separation

SECTION III – POLICE BASIC AND IN-SERVICE TRAINING

Identify prior police basic training. A copy of the curriculum identifying the topics and hours which composed the basic and in-service police training as well as any certificates of completion or official transcripts issued by the entity that conducted the training must be attached. Attach all training you wish to have considered.		
Name of Law Enforcement Agency or Academy that provided police basic training		Telephone
Address		City, State, ZIP
Course Director Name	Course start date	Course end date

ACCEPTABLE DOCUMENTATION

- ☐ A certificate of successful completion from a police basic training course.
or
☐ An official transcript from the training provider of a police basic training course.
or
☐ The course curriculum including topics and hours from a basic training course.
and / or
☐ An official transcript from the training provider of police in-service training courses.
☐ Certificates of successful completion from police in-service training courses.
☐ The course curricula including topics and hours from police in-service training courses.

DCJS USE ONLY

Training Verified By:	Approved By:	Date:	School ID:
Employer Code:	Rank Code:	Course Code:	

New York State Division of Criminal Justice Services
WAIVER OF PEACE OFFICER TRAINING REQUIREMENT
(Executive Law §841)

THIS FORM IS USED BY PERSONS WHO HAVE RECEIVED PRIOR CERTIFICATION OF POLICE BASIC TRAINING FROM THE STATE, A COUNTY, CITY, TOWN, VILLAGE, MUNICIPAL AUTHORITY, OR POLICE DISTRICT OF NEW YORK STATE WHILE FORMERLY EMPLOYED AS A POLICE OFFICER. FORMS PRESENTED FOR FILING MUST CONTAIN ORIGINAL SIGNATURES. ALTHOUGH THE BLANK FORM MAY BE DUPLICATED, PHOTOCOPIES OF COMPLETED FORMS, OR FORMS WITH PHOTOCOPIED SIGNATURES WILL NOT BE ACCEPTED.

Executive Law §841 authorizes the commissioner of the Division of Criminal Justice Services to certify police and peace officer basic training, and to issue equivalency certificates when appropriate.

SECTION I: APPLICANT INFORMATION

This section must be completed by the chief executive officer of the applicant's current employer. Only individuals appointed to positions defined in Criminal Procedure Law Sections 2.10 or 2.16 are eligible to apply for the waiver.

Type or print legibly, the applicant's last name, first name, middle initial, date of birth, social security number, and gender. Enter the name of the current employer, the rank and/or title of the applicant, and the date of initial appointment. While the Social Security Number is not required, the accuracy of linking future training records with appointment information cannot be assured without it. Carefully read the certification. Sign and date in the area provided. With the exception of Social Security Number, the information in Section I is required. Incomplete submissions will not be processed.

SECTION II: PREVIOUS POLICE OR PEACE OFFICER EXPERIENCE

Type or print legibly, the agency name, telephone, complete mailing address, title or rank of the applicant, type of appointment (full or part-time), the date of appointment and the date of separation from service (if any). Repeat for each police employer. Incomplete submissions will not be processed.

Applicants must possess a valid certificate of police basic training to be eligible for the waiver. The provisions of General Municipal Law §209-q regarding the validity of police officer basic training certification applies to former police officers seeking appointment as peace officers, regardless of past employment.

SECTION - III: POLICE BASIC TRAINING

Type or print legibly, the name, telephone, complete mailing address of the agency or academy that provided the police basic training course. Include the name of the course director and the dates of the course. Incomplete submissions will not be processed. **A photocopy of the certificate of completion must be attached.**

MAILING INSTRUCTIONS:

Mail completed forms to:

NYS Division of Criminal Justice Services
Alfred E. Smith State Office Building
Office of Public Safety – Records Unit
80 South Swan St., 3rd Floor
Albany, NY 12210

QUESTIONS:

If you have any questions regarding this form, call (518) 457-2667 for assistance.

New York State Division of Criminal Justice Services
WAIVER OF PEACE OFFICER TRAINING REQUIREMENT
(Executive Law §841)

SECTION I – APPLICANT INFORMATION (To be completed by the chief law enforcement officer)

Applicant Last Name	Applicant First Name	MI	Date of Birth	Social Security Number*	Gender ☐ M ☐ F
Current Employer		Rank or Title		Date of Appointment	
<i>I hereby certify the above named individual has been appointed as a sworn peace officer with this agency. I have determined that he/she has completed the basic training course required by and while employed by the state, a city, town, village, municipal authority, or police district in the state of New York. Accordingly, I request that the Division of Criminal Justice Services records be adjusted to reflect that this officer has met the basic training requirements for appointment of police officers as set forth in section 2.30 of the Criminal Procedure Law, since this training meets or exceeds Municipal Police Training Council requirements for basic training for peace officers. I understand that the information in Section I is part of a written statement that will be presented to the Division of Criminal Justice Services for filing, and I certify that it is true to the best of my knowledge and belief.</i>					
Signature of Chief Executive Officer				Date	

*Pursuant to the New York State Personal Privacy Protection Law, DCJS is authorized to collect personal identifying information as part of a public safety agency record. Personal identifying information on this form shall not be revealed, released, transferred, disseminated or otherwise communicated orally, in writing, or by electronic means other than to the registrant. Disclosure of personal identifying information is voluntary. Refusal to provide personal identifying information shall not result in the denial of any right, benefit, or privilege.

SECTION II – PREVIOUS POLICE OFFICER EXPERIENCE

Identify previous police or peace officer employment. If more space is needed, attach a separate sheet.			
Name of Previous Law Enforcement Employer			Telephone
Address		City, State, ZIP	
Rank or Position	Type of Appointment ☐ Full-time ☐ Part-time	Date of appointment	Date of separation

SECTION III – POLICE BASIC TRAINING

Identify prior police basic training. A copy of the certificate of completion for police basic training issued by the New York State Police, the New York City Police Department or the Municipal Police Training Council must be attached.		
Name of Law Enforcement Agency or Academy		Telephone
Address	City, State, ZIP	
Course Director Name	Course start date	Course end date

DCJS USE ONLY

Training Verified By:	Approved By:	Date:	School ID:
Employer Code:	Rank Code:	Course Code: 988	



NEW YORK STATE
Division of Criminal Justice Services
Office of Public Safety
Security Guard Program

SECURITY GUARD FIREARMS TRAINING QUESTIONNAIRE

In an effort to assess the quality of security guard firearms training being provided by NYS approved armed security guard training schools, the Division of Criminal Justice Services is requesting the completion of this questionnaire.

Name: _____

Date: _____

Signature: _____

Date of Birth: _____

Address: _____

Telephone Number: _____

Are you an employed security guard? Yes ☐ No ☐ Never ☐ No longer employed ☐

Did you complete the 47 Hour Firearms Training Course for Security Guards? Yes ☐ No ☐

If yes, continue

Training began on: Month _____ Day _____ Year _____ and training ended on: Month _____ Day _____ Year _____

Time of training: _____ a.m. to _____ p.m. OR _____ p.m. to _____ p.m.

Name of School: _____

Address of training: _____

Names of instructor(s): _____

How many hours of training did you receive? _____ hours

Did you receive classroom instruction in a classroom? Yes ☐ No ☐

How was the classroom instruction conducted? (Check all that apply) All lecture ☐ Some lecture ☐ All video ☐ Some video ☐

Did you receive instruction on the range? Yes ☐ No ☐

How was the range instruction conducted? (Check all that apply)

All lecture ☐ Some lecture ☐ All video ☐ Some video ☐ Shooting exercises ☐

Did you complete training in the Use of Force/Deadly Physical Force? Yes ☐ No ☐

Did you practice shooting your weapon while on the range? Yes ☐ No ☐

Did you qualify with your weapon and ammunition? Yes ☐ No ☐ Type of weapon used: _____

Were handouts provided? Yes ☐ No ☐ Were you required to take notes? Yes ☐ No ☐

Did you take a final written examination? Yes ☐ No ☐

Did you receive a certificate of completion? Yes ☐ No ☐

Did you complete the 8 Hour Firearms Training Course for Armed Security Guards?

Yes ☐ No ☐

If yes, continue

Date(s) of training: _____ Time of Training: _____ a.m. to _____ p.m. **OR** _____ p.m. to _____ p.m.

Name of School: _____

Address of training: _____

Names of instructor(s): _____

How many hours of training did you receive: _____ hours

Did you receive classroom instruction? Yes ☐ No ☐

How was the classroom instruction conducted? (Check all that apply) All lecture ☐ Some lecture ☐ All video ☐ Some video ☐

Did you receive instruction on the range? Yes ☐ No ☐

How was the range instruction conducted? (Check all that apply)

All lecture ☐ Some lecture ☐ All video ☐ Some video ☐ Shooting exercises ☐

Did you complete training in the Use of Force/Deadly Physical Force? Yes ☐ No ☐

Did you practice shooting your weapon while on the range? Yes ☐ No ☐

Did you qualify with your duty weapon and duty ammunition? Yes ☐ No ☐ Type of weapon used: _____

Were handouts provided? Yes ☐ No ☐ Were you required to take notes? Yes ☐ No ☐

Did you take a final written examination? Yes ☐ No ☐

Did you receive a certificate of completion? Yes ☐ No ☐

Please use the space below to provide any additional information on the security guard training you completed.

Thank you for completing this questionnaire. If you have any questions, please contact the Office of Public Safety, Security Guard Program at (518) 457-4135.

Forward the completed questionnaire either by mail to:

NYS Division of Criminal Justice Services

Office of Public Safety

Security Guard Program

80 South Swan Street

Albany, NY 12210

By fax: (518) 485-7639

Or by e-mail to: Mary.O'Connell@dcjs.state.ny.us



NEW YORK STATE
Division of Criminal Justice Services
Office of Public Safety
Security Guard Program

SECURITY GUARD TRAINING QUESTIONNAIRE

In an effort to assess the quality of security guard training being provided by NYS approved security guard training schools, the Division of Criminal Justice Services is requesting the completion of this questionnaire.

Name: _____

Date: _____

Signature: _____

Date of Birth: _____

Address: _____

Telephone Number: _____

Are you an employed security guard? Yes ☐ No ☐ Never ☐ No longer employed ☐

Did you complete the Eight-Hour Pre-Assignment Training Course for Security Guards? Yes ☐ No ☐

If yes, continue

Date(s) of training: _____ Time of Training: ____ a.m. to ____ p.m. OR ____ p.m. to ____ p.m.

Name of School: _____

Address of training: _____

Names of instructor(s): _____

How many hours of training did you receive? ____ hours

How was the training conducted? (Check all that apply) All Lecture ☐ Some Lecture ☐ All Video ☐ Some Video ☐

Were handouts provided? Yes ☐ No ☐

Were you required to take notes? Yes ☐ No ☐

Did you take a final written examination? Yes ☐ No ☐

Did you receive a certificate of completion? Yes ☐ No ☐

Did you complete the Sixteen Hour On-The-Job Training Course for Security Guards? Yes ☐ No ☐

If yes, continue

Training began on: Month ____ Day ____ Year ____ and finished on: Month ____ Day ____ Year ____

Time of training: ____ a.m. to ____ p.m. OR ____ p.m. to ____ p.m.

Name of School: _____

Address of training: _____

Names of instructor(s): _____

How many hours of training did you receive: ____ hours

How was the training Conducted? (Check all that apply) All lecture ☐ Some Lecture ☐ All Video ☐ Some Video ☐

Did you receive handouts? Yes ☐ No ☐

Were you required to take notes? Yes ☐ No ☐

Did you take a final written examination? Yes ☐ No ☐

Did you receive a certificate of completion? Yes ☐ No ☐

Did you complete the Eight Hour Annual In-Service Training Course for Security Guards? Yes ☐ No ☐

If yes, continue

Date(s) of training: _____ Time of Training: _____ a.m. to _____ p.m. **OR** _____ p.m. to _____ p.m.

Name of School: _____

Address of training: _____

Names of instructor(s): _____

How many hours of training did you receive? _____ hours

Did you receive handouts? Yes ☐ No ☐

How was the training conducted? (Check all that apply) All Lecture ☐ Some Lecture ☐ All Video ☐ Some Video ☐

Were you required to take notes? Yes ☐ No ☐

Did you take a final written examination? Yes ☐ No ☐

Please use the space below to provide any additional information on the security guard training you completed.

Thank you for completing this questionnaire. If you have any questions, please contact the Office of Public Safety, Security Guard Program at (518) 457-4135.

Forward the completed questionnaire either by mail to:

NYS Division of Criminal Justice Services
Office of Public Safety
Security Guard Program
80 South Swan Street
Albany, NY 12210

By fax: (518) 485-7639
Or by e-mail to: Mary.O'Connell@dcjs.state.ny.us

New York State Division of Criminal Justice Services
SECURITY GUARD PROGRAM – ARMORED CAR GUARD TRAINING WAIVER APPLICATION
(General Business Law §89-sss)

THIS FORM IS USED TO APPLY FOR A WAIVER OF REQUIRED INITIAL FIREARMS TRAINING FOR ARMORED CAR GUARDS. FORMS PRESENTED FOR FILING MUST CONTAIN ORIGINAL SIGNATURES. ALTHOUGH THE BLANK FORM MAY BE DUPLICATED, PHOTOCOPIES OF COMPLETED FORMS, OR FORMS WITH PHOTOCOPIED SIGNATURES WILL NOT BE ACCEPTED. OMISSIONS OR LACK OF INFORMATION WILL **STOP** THE APPROVAL PROCESS.

Pursuant to General Business Law §89-sss(4) and (5), the Division of Criminal Justice Services (DCJS) shall waive the training requirements specified with respect to applicants employed by armored car carriers, if the applicant provides appropriate documentation to demonstrate that he or she was or is subject to training requirements which meet or exceed the requirements established pursuant to General Business Law §89-sss(1).

Applicants for an Armored Car Guard Training Waiver must possess a **valid pistol license** pursuant to New York State Penal Law (PL) §400.00, or be exempted from such license pursuant to PL §265.20.

Armed Security Guards who have completed an approved 47 Hour Firearms Training Course for Armed Security Guards may apply for this waiver.

Upon filing this form, **Peace Officers** who have been employed for eighteen months or more and who possess a valid certificate of completion which includes an initial course in firearms and deadly physical force training approved by the Municipal Police Training Council (MPTC) as part of their basic training, and **Police Officers** as defined in Criminal Procedure Law section 1.20(34) shall be **exempt** from the requirements of General Business Law §89-sss(1).

SECTION I: APPLICANT INFORMATION

This section must be completed by the applicant. Only individuals who have completed training listed in Section III of this form may apply for a waiver.

Type or print legibly, the applicant's last name, first name, middle initial, date of birth, Social Security Number, sex, telephone number, address information, and pistol license information. Enter the complete home mailing address, home street address if different, and county of home residence. If the applicant is temporarily living away from home (e.g. enrolled at a college or university, on military assignment, etc.) **DO NOT** list the temporary address. Incomplete submissions will not be processed.

SECTION II - EMPLOYMENT EXPERIENCE

Check the appropriate box(es) and enter the number of years and months worked for any categories being claimed as work experience. **The applicant is required to submit an original letter from the employer verifying employment dates and experience** (sample letter attached). Verification of law enforcement employment will be confirmed through the Police/Peace Officer Registry within the Division of Criminal Justice Services.

If it has been more than 1 year since the completion of initial firearms training, former police or peace officers must submit proof of successful completion of annual firearms training course (completed within twelve months of date of application) which meets or exceeds the standards established by the MPTC or successful completion of the 8 Hour Annual In-Service Training Course for Armed Security Guards.

SECTION III – ARMED SECURITY GUARD FIREARMS TRAINING COURSE

This section is for armed security guard applicants who have completed the 47 Hour Firearms Training Course for Armed Security Guards. Police and peace officer applicants may proceed to section IV.

Enter the dates of firearms training as well as the entity that conducted the training. Enclose a copy of your 47 Hour Firearms Training Course for Armed Security Guards certificate. Training will be confirmed through DCJS training records.

If it has been more than 1 year since the completion of the 47 Hour Firearms Training Course for Armed Security Guards, proof of successful completion of the Eight Hour Annual Firearms Training Course for Armed Security Guards (completed within twelve months of date of application) must be submitted with the waiver application.

New York State Division of Criminal Justice Services
SECURITY GUARD PROGRAM – ARMORED CAR GUARD TRAINING WAIVER APPLICATION
(General Business Law §89-sss)

SECTION IV – ATTESTATION

This is an attestation to the accuracy of information supplied on the application. **This must be signed and sworn to by the applicant before a notary public.** Failure to complete this section will **STOP** the training waiver process.

MAIL APPLICATION TO:

Where applicable, include the following:

- Original letter from employer verifying employment experience and employment dates (see sample letter).
- Course completion certificate or documentation verifying satisfactory completion with dates of course(s) (armed guard applicants).
- Photocopy of valid NYS pistol permit (pursuant to NYS Penal Law §400.00) or peace officer identification card (if applicable).
- Other than this application, **do not submit original documentation** unless specifically requested to do so. Submitted documents will not be returned.

**NYS Division of Criminal Justice Services
Office of Public Safety - Security Guard Program
80 South Swan Street, Albany, NY 12210**

QUESTIONS

If you have any questions regarding this form, call (518) 457-4135 for assistance.

New York State Division of Criminal Justice Services
SECURITY GUARD PROGRAM – ARMORED CAR GUARD TRAINING WAIVER APPLICATION
(General Business Law §89-sss)

Sample employment verification letter, to be submitted **on agency/company letterhead**.

Date

NYS Division of Criminal Justice Services
Office of Public Safety - Security Guard Program
80 South Swan Street, Albany, NY 12210

(Applicant Name) has been continuously employed as **(position)** with the **(department/agency name)** from **(start date)** to **(end date)**. They **(are/are not)** authorized to carry a firearm in the performance of their official duties and has been since **(date armed)**.

Our records indicate **(he/she)** has completed annual training in firearms as of **(date of completion)**.

Sincerely,

Agency/Company CEO
Title

New York State Division of Criminal Justice Services
SECURITY GUARD PROGRAM – ARMORED CAR GUARD TRAINING WAIVER APPLICATION



(General Business Law §89-sss)

SECTION I – APPLICANT INFORMATION

Last Name	First Name	MI	Date of Birth	Social Security Number*
Home Residence Mailing Address		City, State, Postal Code		
Home Residence Mailing Address (if Different)	City, State, Postal Code		Apt./Suite#	County of Home Residence
Home Telephone Number (Area Code First)	Alternate Telephone Number (Area Code First)		Cellular Telephone Number (Area Code First)	

*Pursuant to the New York State Personal Privacy Protection Law, DCJS is authorized to collect personal identifying information as part of a public safety agency record. Personal identifying information on this form shall not be revealed, released, transferred, disseminated or otherwise communicated orally, in writing, or by electronic means other than to the registrant. Disclosure of personal identifying information is voluntary. Refusal to provide personal identifying information shall not result in the denial of any right, benefit, or privilege.

SECTION II – EMPLOYMENT EXPERIENCE

☐ Security Guard Years/mos	☐ Peace Officer (trained and authorized to carry a firearm in the line of duty) Years/mos	☐ Police Officer Years/mos
An original copy of the letter from the employer verifying dates and type of employment must be included.		

SECTION III – ARMED SECURITY GUARD FIREARMS TRAINING COURSE (armed security guard applicants only)

47 Hour Firearms Training Course for Armed Security Guards	From(mm/dd/yyyy)	To (mm/dd/yyyy)	Conducted by:
A copy of the firearms training course completion certificate must accompany the application.			

ATTENTION ALL APPLICANTS

If it has been more than one year since completion of an initial firearms training course, include documentation of completion of an Annual Firearms Training Course or 8 Hour Annual In-service Training Course for Armed Security Guards.

A copy of a valid pistol permit issued in New York State or police or peace officer (as defined in NYS CPL) identification must accompany the application.

SECTION IV – ATTESTATION

Applicant Attestation: *This affidavit must be signed and sworn to by the Applicant before a Notary Public.* I hereby attest that the information provided in this application is true to the best of my knowledge and belief. I understand that any omission or inaccuracy may be deemed sufficient reason to deny approval. I understand that the Division of Criminal Justice Services may ask for additional information/documentation.

Notary Stamp

Applicant Signature

FOR DCJS USE ONLY

FOR DCJS USE ONLY

Reviewed By:

Date:

Sworn and subscribed before me
 this _____ day of _____ 20____

Notary Signature

New York State Division of Criminal Justice Services
SECURITY GUARD PROGRAM – ARMED SECURITY GUARD INSTRUCTOR APPLICATION

THIS FORM IS USED TO APPLY FOR ARMED SECURITY GUARD INSTRUCTOR CERTIFICATION. FORMS PRESENTED FOR FILING MUST CONTAIN ORIGINAL SIGNATURES. ALTHOUGH THE BLANK FORM MAY BE DUPLICATED, PHOTOCOPIES OF COMPLETED FORMS, OR FORMS WITH PHOTOCOPIED SIGNATURES WILL NOT BE ACCEPTED. OMISSIONS OR LACK OF INFORMATION WILL **STOP** THE APPROVAL PROCESS.

Pursuant to the (9)NYCRR 6029.5, this application is used for persons who have a minimum of three years experience as a police officer, peace officer, or armed security guard supervisor or manager and who have successfully completed a DCJS approved civilian or law enforcement **firearms instructor course** and are seeking certification as an Armed Security Guard Instructor. DCJS reserves the right to require further documentation as necessary to properly classify and/or verify the information and experience contained herein.

SECTION I - APPLICANT INFORMATION

Type or print legibly, the applicant's last name, first name, middle initial, date of birth, Social Security Number, sex, address information, telephone number, and any languages spoken (other than English). Check the appropriate box regarding pistol permit and enter the relevant data in the subsequent boxes unless exempted from licensing requirements pursuant to NYS Penal Law §400.00 (police or certain peace officers). If the applicant is temporarily living away from home (e.g. enrolled at a college or university, on military assignment, etc.) **DO NOT** list the temporary address. Incomplete submissions will not be processed.

Applicants for an Armed Security Guard Instructor must possess a valid pistol license pursuant to New York State Penal Law (PL) §400.00, or be exempted from such license pursuant to PL §265.20.

A security guard instructor must meet minimum requirements pursuant to 9 NYCRR Part 6029 to include be an officer, member, or principal currently licensed by the Department of State as a private investigator; watch, guard or patrol agency; or armored car carrier agency; or maintain a valid security guard registration card issued by the Department of State; or maintain a valid armored car guard registration card issued by the Department of State. Enter your UID Number or Department of State License Number on the form.

SECTION II - EDUCATION

Check the appropriate box if you have a high school diploma, equivalency, or neither.

SECTION III - EMPLOYMENT EXPERIENCE

Check the appropriate box(es) and enter the number of years and months worked for any categories being claimed as work experience. Applicants must have held the position of peace officer, police officer, or armed security guard and have carried a firearm in the performance of their duties for a period of at least 3 years. **The applicant is required to submit an original letter from the employer verifying employment dates and experience** (sample letter attached). Verification of law enforcement employment will be confirmed through the Police/Peace Officer Registry within the Division of Criminal Justice Services.

SECTION IV - FIREARMS INSTRUCTOR TRAINING

The applicant must provide the following information for the instructor course **completed**: title (name of course), what entity administered the training, and the course length (number of hours). Enclose a copy of the certificate of completion.

SECTION V - FIREARMS INSTRUCTOR EXPERIENCE

Enter the total number of years as an instructor with a security guard, criminal justice, and/or law enforcement agency or company. List the locations and dates of training you have provided within the last five years. If you require additional space, attach a separate sheet using the same format. Include official documentation which demonstrates your participation in each instance listed.

SECTION VI - ATTESTATION

This is an attestation to the accuracy of information supplied on the application. Indicate whether or not DCJS is authorized to release your contact information on a listing of security guard schools and/or instructors. **This must be signed and sworn to by the applicant before a notary public.** Photocopies of forms or forms with photocopied signatures will not be accepted. Failure to complete this section will **STOP** the application process.

New York State Division of Criminal Justice Services
SECURITY GUARD PROGRAM – ARMED SECURITY GUARD INSTRUCTOR APPLICATION

MAIL APPLICATION TO:

Where applicable, include the following:

- Original letter from employer verifying employment experience and employment dates (see sample letter).
- Course completion certificate or documentation verifying satisfactory completion with dates of firearms instructor course(s).
- A copy of a valid pistol license issued pursuant to NYS penal Law §400.00 or appropriate law enforcement identification.
- Other than this application, **do not submit original documentation** unless specifically requested to do so. Submitted documents will not be returned.

**NYS Division of Criminal Justice Services
Office of Public Safety - Security Guard Program
Alfred E. Smith Office Building
80 South Swan Street
Albany, NY 12210-8002**

QUESTIONS

If you have any questions regarding this form, call (518) 457-4135 for assistance.

New York State Division of Criminal Justice Services
SECURITY GUARD PROGRAM – ARMED SECURITY GUARD INSTRUCTOR APPLICATION

Sample employment verification letter, to be submitted **on agency/company letterhead**.

Date

**NYS Division of Criminal Justice Services
Office of Public Safety - Security Guard Program
Alfred E. Smith Office Building
80 South Swan Street
Albany, NY 12210-8002**

(Applicant Name) has been continuously employed as **(position)** with the **(department/agency name)** from **(start date)** to **(end date)**. They **(are/are not)** authorized to carry a firearm in the performance of their official duties and has been since **(date armed)**.

Our records indicate **(he/she)** has completed annual training in firearms and the use of deadly physical force as of **(date of completion)**.

Sincerely,

Agency/Company CEO
Title

New York State Division of Criminal Justice Services
SECURITY GUARD PROGRAM – ARMED SECURITY GUARD INSTRUCTOR APPLICATION



SECTION I – APPLICANT INFORMATION (to be completed by the applicant)

Last Name	First Name	MI	Date of Birth	Social Security Number*	Sex
Mailing Address	Apt./Suite#	City, State			Postal Code
Home Residence Address (if Different)	Apt./Suite#	City, State, Zip		Postal Code	County of Home Residence
Home Telephone Number (area code first)	UID Number or DOS License Number			Cellular Telephone Number (area code first)	

APPLICANT MUST POSSESS A VALID PISTOL LICENSE PRIOR TO SUBMITTING THIS APPLICATION

*Pursuant to the New York State Personal Privacy Protection Law, DCJS is authorized to collect personal identifying information as part of a public safety agency record. Personal identifying information on this form shall not be revealed, released, transferred, disseminated or otherwise communicated orally, in writing, or by electronic means other than to the registrant. Disclosure of personal identifying information is voluntary. Refusal to provide personal identifying information shall not result in the denial of any right, benefit, or privilege.

SECTION II – EDUCATION

Do you possess a high school diploma or GED? ☐ Diploma ☐ GED ☐ Neither

SECTION III – EMPLOYMENT EXPERIENCE

☐ Security Guard Years/mos	☐ Peace Officer (trained and authorized to carry a firearm in the line of duty) Years/mos	☐ Police Officer Years/mos
An original copy of the letter from the employer verifying dates and type of employment must be included.		

SECTION IV – FIREARMS INSTRUCTOR TRAINING

Course Title	Administered by	Course Length (hours)
A copy of the course completion certificate must accompany the application.		

SECTION V – INSTRUCTOR EXPERIENCE

Enter the total number of years as a firearms instructor with a security, criminal justice and/or law enforcement agency/company. List the agency/company for which you have provided instruction over the last five years. If you require more space, attach additional sheets. Include official documentation which demonstrates your participation in each instance listed.		Number of years
Name of Entity	mm/dd/yyyy	mm/dd/yyyy
Name of Entity	mm/dd/yyyy	mm/dd/yyyy
Name of Entity	mm/dd/yyyy	mm/dd/yyyy

SECTION VI – ATTESTATION

Applicant Attestation: This affidavit must be signed and sworn to by the Applicant before a Notary Public. I hereby attest that the information provided in this application is true to the best of my knowledge and belief. I understand that any omission or inaccuracy may be deemed sufficient reason to deny approval. I understand that the Division of Criminal Justice Services may ask for additional information/documentation.	
I give permission to the Division of Criminal Justice Services (DCJS) to release my name, address and telephone number to those requesting general information on, or a listing of, NYS Certified Security Guard Instructors. ☐ Yes ☐ No	
Notary Stamp	
FOR DCJS USE ONLY FOR DCJS USE ONLY Reviewed By: Date: Applicant Signature	Sworn and subscribed before me this _____ day of _____ 20____ Notary Signature

THIS FORM IS USED TO APPLY FOR THE INITIAL SECURITY GUARD INSTRUCTOR CERTIFICATION. FORMS PRESENTED FOR FILING MUST CONTAIN ORIGINAL SIGNATURES. ALTHOUGH THE BLANK FORM MAY BE DUPLICATED, PHOTOCOPIES OF COMPLETED FORMS, OR FORMS WITH PHOTOCOPIED SIGNATURES WILL NOT BE ACCEPTED. OMISSIONS OR LACK OF INFORMATION WILL **STOP** THE REVIEW PROCESS.

A non-refundable fee of \$500 must be submitted with the Security Guard Instructor Application. Payment must be in the form of a money order, bank certified check, or corporate check and made payable to the NYS Division of Criminal Justice Services (DCJS). A Security Guard Instructor Certification Review Worksheet is included with this application for self evaluation purposes to assist in determining if the application meets all the required information and meets minimum requirement for submission to DCJS. Since the application fee is non-refundable, it is recommended that the applicant complete the Worksheet before submitting the application to DCJS. Questions concerning the completion of the Worksheet should be directed to Security Guard Program staff at (518) 485-2095.

Pursuant to the (9)9 NYCRR 6029.3, this application is used for persons who possess a combination of education, teaching experience, formal instructor training, and law enforcement experience and or security experience and are seeking certification as a Security Guard Instructor. DCJS reserves the right to require further documentation as necessary to properly classify and/or verify the information and experience contained herein.

SECTION I: APPLICANT INFORMATION

Type or print legibly, the applicant's last name, first name, middle initial, date of birth, social security number*, gender, address, and telephone number. If the applicant is temporarily living away from home (e.g. enrolled at a college or university, on military assignment, etc.) **DO NOT** list the temporary address. Check the appropriate box(es) regarding criminal conviction, pending criminal charges, and revocations or denials of any license, permit, commission, registration, or application. If answering yes, submit all relevant documents with application.

A security guard instructor must meet minimum requirements pursuant to 9 NYCRR Part 6029 to include being an officer, member, or principal currently licensed by the Department of State as a private investigator; watch, guard or patrol agency; or armored car carrier agency; or maintain a valid security guard registration card issued by the Department of State; or maintain a valid armored car guard registration card issued by the Department of State. Enter your UID Number or Department of State License Number on the form.

*Pursuant to the New York State Personal Privacy Protection Law, DCJS is authorized to collect personal identifying information as part of a public safety agency record. Personal identifying information on this form shall not be revealed, released, transferred, disseminated, or otherwise communicated orally, in writing, or by electronic means other than to the applicant. Disclosure of personal identifying information is voluntary. Refusal to provide personal identifying information shall not result in the denial of any right, benefit, or privilege.

SECTION II – EDUCATION

Enter the highest grade the applicant has completed, and the area of concentration (if above high school). If you have accumulated 60 or more college credits, but have not completed a college degree program, you may qualify for additional points. Check the appropriate box for Criminal Justice or Security Management/Administration if you have completed a minimum of 24 college credits in either discipline. Enter the number of credits you have earned in Criminal Justice or Security Management/Administration. Attach copies of your degree(s) and or transcript where appropriate.

SECTION III - EMPLOYMENT EXPERIENCE

Check the appropriate box(es) and enter the number of years and months worked for any categories being claimed as work experience. **The applicant is required to submit an original letter from the employer verifying employment dates and experience.** Verification of law enforcement employment will usually be confirmed through the Police/Peace Officer Registry within the Division of Criminal Justice Services.

SECTION IV – INSTRUCTOR TRAINING

The applicant must provide the following information for the instructor course **completed**: title (name of course), what entity administered the training, and the course length (number of hours). Only DCJS approved courses, such as the Instructor Development Course (Methods of Instruction - NYPD), Security Guard Instructor Development Course, or a valid NYS Teachers Certificate.

SECTION V - INSTRUCTOR EXPERIENCE

Enter the total number of years as an instructor with a security guard, criminal justice, and law enforcement agency or company. List the locations and dates of training you provided within the last five years. If you require additional space, attach a separate sheet using the same format.

SECTION VI – APPLICANT AFFIRMATION

This is an affirmation to the accuracy of information supplied on the application. Indicate whether or not DCJS is authorized to release your contact information on a listing of security guard schools and/or instructors. **This must be signed and sworn to by the applicant before a notary public.** Failure to complete this section as required will **STOP** the application process.

Where applicable, include the following:

- Original letter from employer verifying employment experience and employment dates.
- Course completion certificate or documentation verifying satisfactory completion with dates of instructor course(s).
- Other than this application, **do not submit original documentation** unless specifically requested to do so. Submitted documents will not be returned.

MAIL APPLICATION AND PAYMENT TO:

Kimberly Szady, Director of Finance
NYS Division of Criminal Justice Services
Office of Financial Services
Alfred E. Smith Office Building,
80 South Swan Street
Albany, NY 12210

***Do Not Mail Cash, Personal Checks, or Credit Cards**

Sample employment verification letter, to be submitted **on agency/company letterhead**.

Date

NYS Division of Criminal Justice Services
Office of Public Safety - Security Guard Program
AESOB - 80 S. Swan Street
Albany, NY 12210

(Applicant Name) has been continuously employed as **(position)** with the **(department/agency name)** from **(start date)** to **(end date)**.

Sincerely,

Agency/Company CEO
Title

New York State Division of Criminal Justice Services
SECURITY GUARD PROGRAM – SECURITY GUARD INSTRUCTOR APPLICATION

IA

SECTION I – APPLICANT INFORMATION (to be completed by the applicant)

Last Name	First Name	MI	Date of Birth	Social Security Number*	Gender
Home Mailing Address	Apt./Suite#	City, State			Zip Code
Home Residence Address (if Different)	Apt./Suite#	City, State			Zip Code County of Home Residence
Home Telephone Number (area code + number)		Cellular Telephone Number (area code + number)		Department of State License Number or (UID)	
Has the Applicant ever been convicted in this state or elsewhere of a crime or offense that is a misdemeanor or a felony of a crime? ☐ No ☐ Yes If yes, you must submit with this application a written explanation giving the place, court jurisdiction, nature of the offense, sentence and/or other disposition. You must submit a copy of the accusatory instrument (e.g., indictment, criminal information or complaint) and a Certificate of Disposition. If you possess or have received a Certificate of Relief from Disabilities, Certificate of Good Conduct or Executive Pardon, you must submit a copy with this application. Are there any criminal charges (misdemeanors or felonies) pending against you in any court in this state or elsewhere? ☐ No ☐ Yes If yes, you must submit a copy of the accusatory instrument (e.g., indictment, criminal information or complaint). Has any license, permit, commission, registration or application for a license, permit, commission, or registration held by you or a company in which you are or were a principal or employee in New York State or elsewhere ever been revoked, suspended or denied by any state, territory or governmental jurisdiction or foreign country, for any reason? ☐ No ☐ Yes If yes, you must submit all relevant documents, including the agency determination, if any.					

*Pursuant to the New York State Personal Privacy Protection Law, DCJS is authorized to collect personal identifying information as part of a public safety agency record. Personal identifying information on this form shall not be revealed, released, transferred, disseminated or otherwise communicated orally, in writing, or by electronic means other than to the registrant. Disclosure of personal identifying information is voluntary. Refusal to provide personal identifying information shall not result in the denial of any right, benefit, or privilege.

SECTION II – EDUCATION

Highest Grade Completed: ☐ HS/GED ☐ AS ☐ BA/BS ☐ MS/MA ☐ Phd./JD	Area of Concentration
College Credits/Degree in:	Credits
☐ Criminal Justice ☐ Security Management	

SECTION III – EMPLOYMENT EXPERIENCE

☐ Security Guard	Years/Mos	☐ Peace Officer	Years/Mos	☐ Police Officer	Years/Mos	☐ Other (specify) _____	Years/Mos
An original copy of the letter from the employer verifying dates and type of employment must be included.							

SECTION IV – INSTRUCTOR TRAINING (DCJS Approved Instructor courses only)

Course Title	Administered by	Course Length (hours)
A copy of the course completion certificate must accompany the application.		

SECTION V – INSTRUCTOR EXPERIENCE

Enter the total number of years as an instructor with a security, criminal justice and/or law enforcement agency/company. List the agency/company for which you have provided instruction over the last five years. If you require more space, attach additional sheets. Include official documentation which demonstrates your participation in each instance listed.		Years
Name of Entity	mm/dd/yyyy	mm/dd/yyyy
Name of Entity	mm/dd/yyyy	mm/dd/yyyy
Name of Entity	mm/dd/yyyy	mm/dd/yyyy
An original copy of the letter from the employer verifying dates and type of instruction must be included.		

SECTION VI – APPLICANT AFFIRMATION

Applicant Affirmation: This affidavit must be signed and sworn to by the Applicant before a Notary Public. I hereby attest that the information provided in this application is true to the best of my knowledge and belief. I understand that any omission or inaccuracy may be deemed sufficient reason to deny approval. I understand that the Division of Criminal Justice Services may ask for additional information/documentation. I give permission to the Division of Criminal Justice Services (DCJS) to release my name, address and telephone number to those requesting general information on, or a listing of, NYS Certified Security Guard Instructors. ☐ Yes ☐ No	
_____ Applicant Signature	Notary Stamp
FOR DCJS USE ONLY Reviewed By: _____	FOR DCJS USE ONLY Sworn and subscribed before me this ____ day of _____ 20__ _____ Notary Signature

SECURITY GUARD PROGRAM – SECURITY GUARD INSTRUCTOR APPLICATION REVIEW WORKSHEET

This Security Guard Instructor Review Worksheet is for completion by the applicant for **self evaluation purposes** to assist in determining if the application contains all the required information and meets minimum requirements for submission to the Division of Criminal Justice Services (DCJS). The applicant must have a minimum cumulative total of 70 points to be considered for approval as a security guard instructor. A non-refundable fee of \$500 must be submitted with the application. Since the **application fee is non-refundable**, it is recommended that the applicant complete the worksheet before submitting the application to DCJS.

***REFER TO THE INSTRUCTIONS FOR DETAILED INFORMATION ON COMPLETING THE APPLICATION.**

SECTIONS I-IV – Applicant Information, Education, Employment Experience, Instructor Training and Instruction Experience

Is the original copy of the letter from the employer verifying dates and type of employment included with the application?

YES ☐ NO ☐

Is a copy of the course completion certificate included with the application if it is a DCJS approved instructor course?

YES ☐ NO ☐

Has all applicable information been provided in these sections?

YES ☐ NO ☐

SECTION VI – Applicant Affirmation

Is an answer provided for the release of your information on the Instructor Listing?

YES ☐ NO ☐

Is the application signed, dated, and sworn to by the applicant before a Notary Public?

YES ☐ NO ☐

APPLICATION FEE

Is the \$500 non-refundable application fee included with the application?

YES ☐ NO ☐

THE APPLICANT MUST HAVE A MINIMUM CUMULATIVE TOTAL OF 70 POINTS TO BE CONSIDERED FOR APPROVAL AS A SECURITY GUARD INSTRUCTOR. Complete the section below to determine the number of points you will receive from DCJS for your education, employment experience, instructor training and instructor experience **as documented on the application.**

EDUCATION

Number of Points

ADD POINTS FOR ONLY HIGHEST LEVEL OF EDUCATION COMPLETED

(This should be 25, 30, 35, **OR** 40 points. Do not add points together in this section.)

College – 2 years or more without specialization in Law Enforcement or Security, add 25 points

College – 2 years or more with specialization in Law Enforcement or Security, add 30 points

College – 4 years or more without specialization in Law Enforcement or Security, add 35 points

College – 4 years or more with specialization in Law Enforcement or Security, add 40 points

SECURITY GUARD PROGRAM – SECURITY GUARD INSTRUCTOR APPLICATION REVIEW WORKSHEET

EMPLOYMENT EXPERIENCE

Number of Points

If you have police, peace, or security guard industry experience add 10 points for each year of experience up to a maximum of three years. You may not receive more than 30 points.

INSTRUCTOR TRAINING

If you have completed a DCJS approved formal instructor course in the techniques of organizing and presenting instructional materials add 30 points.

INSTRUCTOR EXPERIENCE

If you have documented experience as an instructor in law enforcement or security related subjects add 10 points.

TOTAL NUMBER OF POINTS

Add the number of points for education, employment experience, instructor training and instructor experience for total number of points.

TOTAL NUMBER OF POINTS

***Do not submit application if total number of points is less than 70 points.**



THIS FORM IS USED TO APPLY FOR RENEWAL OF SECURITY GUARD INSTRUCTOR CERTIFICATION. FORMS PRESENTED FOR FILING MUST CONTAIN ORIGINAL SIGNATURES. ALTHOUGH THE BLANK FORM MAY BE DUPLICATED, PHOTOCOPIES OF COMPLETED FORMS, OR FORMS WITH PHOTOCOPIED SIGNATURES WILL NOT BE ACCEPTED. OMISSIONS OR LACK OF INFORMATION WILL **STOP** THE APPROVAL PROCESS.

A \$250 non-refundable fee must be submitted for each certification renewal. If applying for renewal as a security guard instructor, the application fee is \$250. If applying for renewal as an armed security guard instructor, the application fee is \$250. If applying for renewal as a security guard instructor AND armed security guard instructor, the application fee is \$500. Payment must be in the form of a money order, bank certified check, or corporate check and made payable to the NYS Division of Criminal Justice (DCJS).

Pursuant to the (9)NYCRR 6029.3, this application is used for persons who, or possess a combination of education, teaching experience, formal instructor training, and law enforcement experience and or security experience and are seeking certification as a Security Guard Instructor. DCJS reserves the right to require further documentation as necessary to properly classify and/or verify the information and experience contained herein.

SECTION I: APPLICANT INFORMATION

Type or print legibly, the applicant's last name, first name, middle initial, date of birth, *social security number, gender, address, and telephone number. If the applicant is temporarily living away from home, (e.g. enrolled at a college or university, on military assignment, etc.) **DO NOT** list the temporary address. Check the type of instructor certification renewal (general topics, firearms, or both). If applying for the renewal of firearms instructor certification, the applicant must submit documentation verifying instruction of a DCJS approved firearm(s) training course within the last five years. Approved firearms courses include the 47 Hour Firearms Training Courses for police and peace officers and security guards; and the Annual Firearms Courses for peace officers and security guards. If applicable, a copy of the firearms license must be submitted. Check the appropriate box(es) regarding criminal conviction, pending criminal charges, and revocations or denials of any license, permit, commission, registration, or application. If answering yes to any of the questions, contact DCJS staff at 518-485-2095 before submission of the application. Incomplete submissions will not be processed.

A security guard instructor must meet minimum requirements pursuant to 9 NYCRR Part 6029 to include be an officer, member, or principal currently licensed by the Department of State as a private investigator; watch, guard or patrol agency; or armored car carrier agency; or maintain a valid security guard registration card issued by the Department of State; or maintain a valid armored car guard registration card issued by the Department of State. Enter your UID Number or Department of State License Number on the form.

*Pursuant to the New York State Personal Privacy Protection Law, DCJS is authorized to collect personal identifying information as part of a public safety agency record. Personal identifying information on this form shall not be revealed, released, transferred, disseminated, or otherwise communicated orally, in writing, or by electronic means other than to the applicant. Disclosure of personal identifying information is voluntary. Refusal to provide personal identifying information shall not result in the denial of any right, benefit, or privilege.

SECTION II – APPLICANT AFFIRMATION

This is an affirmation to the accuracy of information supplied on the application. Indicate whether or not DCJS is authorized to release your contact information on a listing of security guard schools and/or instructors. **This must be signed and sworn to by the applicant before a notary public.** Failure to complete this section as required will **STOP** the application process.

MAIL APPLICATION AND PAYMENT TO:

Kimberly Szady, Director of Finance
NYS Division of Criminal Justice Services
Alfred E. Smith Office Building
80 South Swan Street
Albany, NY 12210

*Do Not Mail Cash, Personal Checks, or Credit Cards

QUESTIONS

If you have any questions regarding this form, call (518) 485-2095 for assistance.

New York State Division of Criminal Justice Services
SECURITY GUARD PROGRAM – SECURITY GUARD INSTRUCTOR RENEWAL APPLICATION



SECTION I – APPLICANT INFORMATION (to be completed by the applicant)

Last Name	First Name	MI	Date of Birth	*Social Security Number	Gender
Home Mailing Address	Apt./Suite#	City, State			Zip Code
Home Residence Address (if Different)	Apt./Suite#	City, State			Zip Code If applicable, firearms license No.
Home Telephone Number (area code + number)	Department of State License Number or (UID)		General Topics ☐ Firearms ☐		

Has the Applicant ever been convicted in this state or elsewhere of a crime or offense that is a misdemeanor or a felony of a crime? ☐ No ☐ Yes
If yes, you must submit with this application a written explanation giving the place, court jurisdiction, nature of the offense, sentence and/or other disposition. You must submit a copy of the accusatory instrument (e.g., indictment, criminal information or complaint) and a Certificate of Disposition. If you possess or have received a Certificate of Relief from Disabilities, Certificate of Good Conduct or Executive Pardon, you must submit a copy with this application.

Are there any criminal charges (misdemeanors or felonies) pending against you in any court in this state or elsewhere? ☐ No ☐ Yes
If yes, you must submit a copy of the accusatory instrument (e.g., indictment, criminal information or complaint).

Has any license, permit, commission, registration or application for a license, permit, commission, or registration held by you or a company in which you are or were a principal or employee in New York State or elsewhere ever been revoked, suspended or denied by any state, territory or governmental jurisdiction or foreign country, for any reason? ☐ No ☐ Yes

If yes, you must submit all relevant documents, including the agency determination, if any.

*Pursuant to the New York State Personal Privacy Protection Law, DCJS is authorized to collect personal identifying information as part of a public safety agency record. Personal identifying information on this form shall not be revealed, released, transferred, disseminated or otherwise communicated orally, in writing, or by electronic means other than to the registrant. Disclosure of personal identifying information is voluntary. Refusal to provide personal identifying information shall not result in the denial of any right, benefit, or privilege.

SECTION II: APPLICANT AFFIRMATION

Applicant Affirmation: This affidavit must be signed and sworn to by the Applicant before a Notary Public. I hereby affirm, under penalties of perjury, that the information provided in this application is true to the best of my knowledge and belief. I understand that any material misstatement may be deemed sufficient reason to deny approval, or may result in the suspension or revocation of my instructor certification, if issued. I further understand that the Division of Criminal Justice Services (DCJS) may ask for additional information/documentation.

I give permission to the Division of Criminal Justice Services to release my name, address and telephone number to those requesting general information on, or a listing of, NYS Certified Security Guard Instructors.

☐ Yes ☐ No

Notary Stamp

 Applicant Signature

Sworn and subscribed before me
 this _____ day of _____ 20_____

FOR DCJS USE ONLY

Reviewed By: _____

Date _____

Notary Signature _____



THIS FORM IS USED TO APPLY FOR APPROVAL OF A SECURITY GUARD TRAINING SCHOOL. FORMS PRESENTED FOR FILING MUST CONTAIN ORIGINAL SIGNATURES. THE BLANK FORM MAY BE DUPLICATED, HOWEVER PHOTOCOPIES OF COMPLETED FORMS, OR FORMS WITH PHOTOCOPIED SIGNATURES WILL NOT BE ACCEPTED. TYPE ALL INFORMATION. OMISSIONS OR LACK OF INFORMATION WILL STOP THE REVIEW PROCESS. THE SCHOOL DIRECTOR WILL BE REQUIRED TO ATTEND AN ORIENTATION SEMINAR IN ALBANY.

Security Guard Training Schools must be approved by the Division of Criminal Justice Services (DCJS), pursuant to Title 9 of the Official Compilation of Codes, Rules, and Regulations of New York State, Part 6028. **Security Guard Training Schools are approved to conduct either mandated non-firearms security guard training, mandated security guard firearms training, or both.**

The process for applying to establish a security guard school consists of the three types of documentation listed below. The documentation is discussed in detail in the following material.

- I. Application
- II. Forms and Documentation
- III. School Prepared Forms

DCJS reserves the right to require further documentation as necessary to properly identify school owners and school directors, verify contact information and determine whether the school location meets DCJS standards for classroom instruction.

A non-refundable fee of \$1000 must be submitted with the Security Guard School Application. Payment must be in the form of a money order, bank certified check, or corporate check and made payable to the NYS Division of Criminal Justice Services (DCJS).

*Pursuant to the New York State Personal Privacy Protection Law, DCJS is authorized to collect personal identifying information as part of a public safety agency record. Personal identifying information on this form shall not be revealed, released, transferred, disseminated, or otherwise communicated orally, in writing, or by electronic means other than to the applicant. Disclosure of personal identifying information is voluntary. Refusal to provide personal identifying information shall not result in the denial of any right, benefit, or privilege.

The applicant will receive the school's approval, or a letter detailing the reason for denial of the application within 120 days of receipt of a complete application. A complete application must contain all information and supporting documentation as outlined below. All of the information requested must be submitted, or the application will be denied.

SECTION I: SCHOOL APPLICATION INFORMATION

TYPE OF TRAINING FOR WHICH APPLICATION IS BEING MADE: Check the type of security guard training the school is applying for. If applying to conduct both types of training, check both boxes.

1. **School Name** – This is the name your school will be utilizing and which will appear on your approval certificate issued by DCJS. If the name of the school is other than your own legal name, the name must be registered. Before filing your Business Certificate as a Sole Proprietor or Partnership, the County Clerk's Office will make a determination of name availability. The Department of State will make a determination on name availability for a corporation, foreign corporation, limited liability company, limited liability partnership, and a limited partnership.
2. **Federal Tax Identification Number or Employer Identification Number** – The school owner (applicant) 9-digit number from the Internal Revenue Service that identifies the school as a business entity.
3. **School Mailing Address** - Provide the mailing address of the school.
4. **School Training Site Address** – This is the address where mandated security guard training courses will be conducted. The training site must have a local certificate of occupancy approving its use for "school purposes" as well as approval from the fire authorities in the jurisdiction where the site is located. DCJS requires that 16 square feet be allotted per student. A determination of the number of students allowed in each training session will be made by DCJS based on the square footage of the classroom and equipment etc. located in the space. You may leave this blank if you have not yet rented the training site. However, the site must be rented upon notice to you by DCJS that your approval is nearing completion and a certificate of occupancy must be provided for final approval. For identification purposes you must provide DCJS with the city where the proposed school is located. **You must complete the Request for Approval of a Training Site for this address.**
5. **Handicap Accessibility** - The training site utilized for mandated non-firearms security guard training must be handicap accessible. Title III of the American with Disabilities Act (effective January 26, 1992), requires private businesses to be accessible to persons with disabilities. The applicant must provide digital photographs of the handicap accessibility elements of the building.
6. **Type of Owner of School** – Proprietorship, partnership, corporation, Not for Profit Corporation, public or private collegiate educational institution, public or private educational institution, governmental agency/entity, or other.

7. **Name of School Owner or Corporation (Applicant), contact and other required information** – If corporation, this should be exactly as it appears on your Certificate of Incorporation. Enter contact information. If sole owner (proprietor), enter your gender, date of birth, and *social security number. The school owner must meet minimum requirements pursuant to 9 NYCRR Part 6028 to include being an officer, member, or principal currently licensed by the Department of State as a private investigator; watch, guard or patrol agency; or armored car carrier agency; or maintain a valid security guard registration card issued by the Department of State; or maintain a valid armored car guard registration card issued by the Department of State.
- 7a. **Affiliation with another school** – The school owner, whose name appears on the application, must answer whether they have ever been affiliated with or owned another proprietary school. If yes, full details of such association, including any fiscal disallowances, fine or penalty, or any other disciplinary action against them or the school by any Local, State or Federal authorities must be provided on a separate sheet.
- 7b. **Disclosure** – The school owner whose name appears on the application must state whether they:
- Have ever been convicted in this state or elsewhere of a crime or offense that is a misdemeanor or a felony. **If yes**, a written explanation giving the place, sentencing court, nature of the offense, sentence and/or other disposition, a copy of the accusatory instrument (e.g. indictment, criminal information, or complaint) and a Certificate of Disposition must be submitted with the application. A Certificate of Relief from Disabilities, Certificate of Good Conduct or Executive Pardon, if applicable, must be submitted with the application.
 - Have any criminal charges (misdemeanors or felonies) pending against them. **If yes**, a copy of the accusatory instrument (e.g. indictment, criminal information, or complaint) must be submitted with the application.
 - Has any license, permit, commission, registration, approval, or application for a license, permit, commission, approval, or registration held by them or a company in which they are or were a principal or employee in New York State or elsewhere ever been revoked, suspended, or denied by any state, territory, or governmental jurisdiction or foreign country, for any reason. **If yes**, submit any relevant documents, including the agency determination.
8. **Name of School Director, contact and other required information** – Enter the name, contact information, gender and social security number of the of the school director. The school director must meet minimum requirements pursuant to 9 NYCRR Part 6028 to include being an officer, member, or principal currently licensed by the Department of State as a private investigator; watch, guard or patrol agency; or armored car carrier agency; or maintain a valid security guard registration card issued by the Department of State; or maintain a valid armored car guard registration card issued by the Department of State.
- 8a. **Affiliation with another school** – The school director, whose name appears on the application, must answer whether they have ever been affiliated with or owned another proprietary school. If yes, full details of such association, including any fiscal disallowances, fine or penalty, or any other disciplinary action against them or the school by any Local, State or Federal authorities must be provided on a separate sheet.
- 8b. **Disclosure** – The school director whose name appears on the application must state whether they:
- Have ever been convicted in this state or elsewhere of a crime or offense that is a misdemeanor or a felony. **If yes**, a written explanation giving the place, court jurisdiction, nature of the offense, sentence and/or other disposition, a copy of the accusatory instrument (e.g. indictment, criminal information, or complaint) and a Certificate of Disposition must be submitted with the application. A Certificate of Relief from Disabilities, Certificate of Good Conduct or Executive Pardon, if applicable, must be submitted with the application.
 - Have any criminal charges (misdemeanors or felonies) pending against them. **If yes**, a copy of the accusatory instrument (e.g. indictment, criminal information, or complaint) must be submitted with the application.
 - Has any license, permit, commission, registration, approval, or application for a license, permit, commission, approval, or registration held by them or a company in which they are or were a principal or employee in New York State or elsewhere ever been revoked, suspended, or denied by any state, territory, or governmental jurisdiction or foreign country, for any reason. **If yes**, submit any relevant documents, including the agency determination.
9. **Name of School Co-Director (if applicable), contact and other required information** – Enter the name, contact information, gender and social security number of the school co-director. There is no requirement that an applicant have a co-director. The school co-director must meet minimum requirements pursuant to 9 NYCRR Part 6028 to include being an officer, member, or principal currently licensed by the Department of State as a private investigator; watch, guard or patrol agency; or armored car carrier agency; or maintain a valid security guard registration card issued by the Department of State; or maintain a valid armored car guard registration card issued by the Department of State.

SECURITY GUARD PROGRAM – SECURITY GUARD TRAINING SCHOOL APPLICATION**SA**

9a. **Affiliation with another school** – The school co-director, whose name appears on the application, must answer whether they have ever been affiliated with or owned another proprietary school. If yes, full details of such association, including any fiscal disallowances, fine or penalty, or any other disciplinary action against them or the school by any Local, State or Federal authorities must be provided on a separate sheet.

9b. **Disclosure** – The school co-director whose name appears on the application must state whether they:

- Have ever been convicted in this state or elsewhere of a crime or offense that is a misdemeanor or a felony. **If yes**, a written explanation giving the place, court jurisdiction, nature of the offense, sentence and/or other disposition, a copy of the accusatory instrument (e.g. indictment, criminal information, or complaint) and a Certificate of Disposition must be submitted with the application. A Certificate of Relief from Disabilities, Certificate of Good Conduct or Executive Pardon, if applicable, must be submitted with the application.
- Have any criminal charges (misdemeanors or felonies) pending against them. **If yes**, a copy of the accusatory instrument (e.g. indictment, criminal information, or complaint) must be submitted with the application.
- Has any license, permit, commission, registration, approval, or application for a license, permit, commission, approval, or registration held by them or a company in which they are or were a principal or employee in New York State or elsewhere ever been revoked, suspended, or denied by any state, territory, or governmental jurisdiction or foreign country, for any reason. **If yes**, submit any relevant documents, including the agency determination.

10. **Partners** – If the ownership is a partnership, enter the name of the partner(s), social security number, date of birth, and contact information. Indicate whether they have ever been affiliated with or owned another proprietary school. If yes, provide full details attached to this application, including any disallowances, fines, denial of license or approval, or any disciplinary action against them or the school by any local, state, or Federal authorities.

10a. **Affiliation with another school** – The applicant must answer for each partner whose name appears on the application, whether they have ever been affiliated with or owned another proprietary school. If yes, full details of such association, including any fiscal disallowances, fine or penalty, or any other disciplinary action against them or the school by any Local, State or Federal authorities must be provided on a separate sheet.

10b. **Disclosure** – The applicant must answer for each partner whose name appears on the application, whether they:

- Have ever been convicted in this state or elsewhere of a crime or offense that is a misdemeanor or a felony. **If yes**, a written explanation giving the place, court jurisdiction, nature of the offense, sentence and/or other disposition, a copy of the accusatory instrument (e.g. indictment, criminal information, or complaint) and a Certificate of Disposition must be submitted with the application. A Certificate of Relief from Disabilities, Certificate of Good Conduct or Executive Pardon, if applicable, must be submitted with the application.
- Have any criminal charges (misdemeanors or felonies) pending against them. **If yes**, a copy of the accusatory instrument (e.g. indictment, criminal information, or complaint) must be submitted with the application.
- Have had any license, permit, commission, registration, approval, or application for a license, permit, commission, approval, or registration held by them or a company in which they are or were a principal or employee in New York State or elsewhere ever revoked, suspended, or denied by any state, territory, or governmental jurisdiction or foreign country, for any reason. **If yes**, submit any relevant documents, including the agency determination.

11. **Audio/Visual Equipment** – Identify the type of audio/visual equipment to be used by the school.

12. **Shipping Information** - In order to provide mandated security guard training, security guard training schools must utilize Optical Mark Reader (OMR) forms for submission of training information to DCJS. These forms are provided by DCJS; however the school is responsible for the cost associated with the shipment of the forms. Enter the name and account number of the shipping company to be used for shipment of Optical Mark Reader forms.

13. **Firearms Training Facility** – To be completed by applicant applying for approval to conduct firearms training. Enter the name of the range and street address (do not enter a post office box), city, state, zip code, county and business telephone number, and type of range (outdoor or indoor facility). Enter the name and telephone number of the contact person for the firearms facility. **You must complete the Request for Approval of Training Site form for this address.** Refer to Section II for additional information.

14. **Certified Security Guard Instructors** - Enter the names of ALL DCJS certified security guard instructor(s) or armed security guard instructor(s) to be utilized by your school. All instructors must possess a valid certification. Instructor certifications are valid for a period of five years, at which time the instructor must apply for renewal. Application to conduct firearms training requires a minimum of one DCJS certified armed security guard instructor. Application to conduct non-firearms security guard training requires a minimum of one DCJS certified security guard instructor.

Enter the social security number, name of instructor as it appears on the certification letter, and type of certification. Check all that apply, GT for General Topics Instructor, FA for Firearms/Armed Security Guard Instructor.

15. **Applicant Affirmation** – This is an affirmation to the accuracy of information provided on the application, an acknowledgment related to General Business Law section 89-n and the NYS Official Compilation of Codes, Rules and Regulations, and that the school director is required to attend an orientation seminar. This must be signed and sworn to by the applicant, school director, and school co-director (if applicable) before a notary public.

SECTION II: FORMS AND DOCUMENTATION

1. **Type of Ownership** – Applicants must provide supporting documents with application for type of ownership. If the type of ownership checked on the application is “Other”, provide applicable documentation.
- a. Sole Proprietorship – Provide consent to do business from county clerk
 - b. Partnership – Provide copy of partnership agreement
 - c. Corporation – Provide Certificate of Incorporation and if applicable, certificate of assumed name
2. **Certificate of Occupancy** – Issued by the municipality in which the training site is located to verify that the training site address is approved for use as a school. A valid Certificate of Occupancy must be included with the application. The address on the certificate must be the same address listed in Number 4 (Training Site) on the application. In some circumstances the applicant may not yet have rented the training site. If this is the case, the Certificate of Occupancy may be missing from the application packet. However, the training site must be rented upon notice to you by DCJS that your approval is nearing completion and a Certificate must be provided for final approval.

A Certificate of Occupancy (CO) is issued by local municipalities to verify that local building codes have been met and the building is suitable for occupancy. It further states the purpose for which the quarters are to be used (i.e., commercial, residential, school, etc.)

To obtain a copy of a CO in NYC, visit the Department of Buildings' Customer Service Counter in your borough office or log on to the Building Information System at <http://nyc.gov/bis>. If a building was constructed before 1938 and there has been no change in use or additions to the property, it may not have a CO. To obtain proof of the legal use of a building that does not have a CO, you must obtain a “Letter of No Objection” from the Department of Buildings' borough office where the property is located. **Applicant must submit a “Letter of No Objection” should the building not have a CO.**

*A Certificate of Occupancy is required for all training sites; however, certain enterprises may be waived from the requirement that the CO specifically approve the site for school use.

**Submission of a Certificate of Occupancy may be waived for governmental agencies or municipalities and public or private secondary or collegiate-level educational institutions in NY or any other jurisdiction.

***If a municipality does not issue COs for existing structures, you must submit a letter from the municipality to that effect.

3. **Zoning Compliance Letter** – Submit proof that the site to be used to conduct training conforms with local zoning laws and regulations. The address in the letter must be the same address listed in Number 4 (Training Site) on the application.

*A Zoning Compliance Letter is required for all training sites; however, certain enterprises may be waived from the requirement that the Zoning Compliance Letter specifically approve the site for school use.

**Submission of a Zoning Compliance Letter may be waived for governmental agencies or municipalities and public or private secondary or collegiate-level educational institutions in NY or any other jurisdiction.

4. **Proof of Insurance for the conduct of firearms training** – An applicant applying for approval to conduct firearms training which is self-insured must submit a Certificate of Insurance evidencing comprehensive general liability coverage from an insurance agency licensed to do business in New York State or procured by a duly licensed excess line broker pursuant to §2118 of the NYS Insurance Law in the minimum amount of \$100,000 per occurrence and \$300,000 in the aggregate which amount shall be available for the payment of claims. The applicant must provide a copy of the Certificate of Insurance. In some circumstances the applicant may not yet have purchased liability insurance. If this is the case, the Certificate of Insurance may be missing from the application packet. However, it must be submitted upon notice to you by DCJS that your approval is nearing completion and the Certificate must be provided for final approval of the application.

New York State Division of Criminal Justice Services
SECURITY GUARD PROGRAM – SECURITY GUARD TRAINING SCHOOL APPLICATION

SA

5. **Fire Authority Approval** - The premises in which mandated security guard training courses will be conducted must be approved for occupancy by the fire authority of the municipality or county in which the site is located. The approval must have been granted during the past three (3) years. The address listed on the fire authority approval must be the same as the address listed in Number 4 (Training Site) of the application. In some circumstances the applicant may not yet have rented the premises. If this is the case, the approval may be missing from the application packet. However, the premises must be rented upon notice to you by DCJS that your approval is nearing completion and Fire Authority Approval must be provided for final approval of the application.
6. **Request for Approval of a Training Site** – A Request for Approval of Training Site form must be completed for the address listed in Number 4 (Training Site) of the application. If the school has more than one training site, the form must be completed for each site. A floor plan must be submitted for the address listed in Number 4 (Training Site) of the application and for any additional training sites. The plan must be drawn to scale of at least ¼" equaling 1". All standard architectural features such as windows, doors, and permanent fixtures should be clearly labeled. The room number, all dimensions, and the use of each room or space must also be clearly labeled. Digital photographs of the exterior of the premises, building handicap accessibility elements and interior rooms identified on the floor plan must be submitted with the floor plan. Digital photos must be submitted on a CD/DVD disk or USB flash drive. In some instances the applicant may have not rented the premises. If this is the case, the photographs and floor plan may be missing from the application packet. However, the premises must be rented upon notice to you by DCJS that your approval is nearing completion and the photographs and floor plan must be provided for final approval of the application. **DCJS reserves the right to inspect the training site prior to approval.**

*Submission of the floor plan may be waived for governmental agencies or municipalities and public or private secondary or collegiate-level educational institutions in NY or any other jurisdiction.

SECTION III: SCHOOL PREPARED FORMS

Approved security guard schools are required to have the following forms. Forms may be in a printer's proof format until approval to print the forms is received from DCJS.

1. Printed catalogue or booklet of mandated security guard training courses to be offered by the school. The catalogue must include a description of each course, when the courses are to be completed (i.e. 16 Hour On-the Job Training Course must be completed within 90 days of employment), school attendance policy (policy must be compliant with NYCRR Part 6027) and the school's refund policy;
2. Printed enrollment agreement. The enrollment agreement must include a refund policy statement. Agents/employees of the school that enroll students must be identified on the enrollment agreement by printed name and signature; and
3. Payment Receipt Form - for issuance to students for verification of payment. The form must identify how payment was made (e.g. cash, check, credit card etc.) and the school name must appear on the receipt form.

MAIL APPLICATION, DOCUMENTATION AND PAYMENT TO:

Kimberly Szady, Director of Finance
NYS Division of Criminal Justice Services
Alfred E. Smith Office Building
80 South Swan Street
Albany, NY 12210

***Do Not Mail Cash, Personal Checks, or Credit Cards**



New York State Division of Criminal Justice Services
SECURITY GUARD PROGRAM – SECURITY GUARD TRAINING SCHOOL APPLICATION

SA

SECTION I: TRAINING SCHOOL INFORMATION

TYPE OF TRAINING: ☐ **SECURITY GUARD TRAINING (NON-FIREARMS)** ☐ **FIREARMS SECURITY GUARD TRAINING**

1. School Name		2. Federal Tax ID Number/Employer ID Number		FOR DCJS USE - School Code	
3. School Mailing Address				Room/Suite	
City, State, Zip Code				County	
4. Training Site Street Address (if different from school mailing address)				Training Site Room/Suite	
Training Site City, State, Zip Code				Training Site County	
Telephone Number (area code + number)			Facsimile Number (area code + number) (optional)		
5. Handicap Accessible Yes ☐ No ☐		6. Type of Ownership of School (check one) Proprietorship ☐ Partnership ☐ Corporation ☐ Not for Profit Corporation ☐ public or private collegiate education institution ☐ public or private education institution ☐ governmental agency/entity ☐ Other (provide type) ☐ _____			
7. School Owner or Corporation Name and Dept. of State License Number or UID			Owner's Name and Title		
Street Address		City, State, Zip Code		Telephone Number (area code + number)	
If sole owner (proprietor) of school provide the following:					
Gender		Date of Birth		*Social Security Number	
				Email Address	
7a. Has the SCHOOL OWNER ever been affiliated with or owned another proprietary school? ☐ No ☐ Yes If yes , please provide full details attached to this application, including any disallowances, fines, or any other disciplinary action against them or the school by any Local, State or Federal authorities.					
7b. Has the SCHOOL OWNER ever been convicted in this state or elsewhere of a crime, misdemeanor or a felony? ☐ No ☐ Yes If yes , you must submit with this application a written explanation giving the place, court jurisdiction, nature of the offense, sentence and/or other disposition. You must submit a copy of the accusatory instrument (e.g., indictment, criminal information or complaint) and a Certificate of Disposition. If you possess or have received a Certificate of Relief from Disabilities, Certificate of Good Conduct or Executive Pardon, you must submit a copy with this application. Are there any criminal charges (misdemeanors or felonies) pending against you in any court in this state or elsewhere? ☐ No ☐ Yes If yes , you must submit a copy of the accusatory instrument (e.g., indictment, criminal information or complaint). Has any license, permit, commission, registration or application for a license, permit, commission, or registration held by you or a company in which you are or were a principal or employee in New York State or elsewhere ever been revoked, suspended or denied by any state, territory or governmental jurisdiction or foreign country, for any reason? ☐ No ☐ Yes If yes , you must submit all relevant documents, including the agency determination, if any.					
8. School Director's Name			Gender		*Social Security Number
Telephone Number (area code + number)		Email Address (REQUIRED)		Department of State License Number or UID	
8a. Has the SCHOOL DIRECTOR ever been affiliated with or owned another proprietary school? ☐ No ☐ Yes If yes , please provide full details attached to this application, including any disallowances, fines, or any other disciplinary action against them or the school by any Local, State or Federal authorities.					

New York State Division of Criminal Justice Services
SECURITY GUARD PROGRAM – SECURITY GUARD TRAINING SCHOOL APPLICATION

SA

8b. Has the SCHOOL DIRECTOR ever been convicted in this state or elsewhere of a crime, misdemeanor or felony? ☐ No ☐ Yes If yes, you must submit with this application a written explanation giving the place, court jurisdiction, nature of the offense, sentence and/or other disposition. You must submit a copy of the accusatory instrument (e.g., indictment, criminal information or complaint) and a Certificate of Disposition. If you possess or have received a Certificate of Relief from Disabilities, Certificate of Good Conduct or Executive Pardon, you must submit a copy with this application. Are there any criminal charges (misdemeanors or felonies) pending against you in any court in this state or elsewhere? ☐ No ☐ Yes If yes, you must submit a copy of the accusatory instrument (e.g., indictment, criminal information or complaint). Has any license, permit, commission, registration or application for a license, permit, commission, or registration held by you or a company in which you are or were a principal or employee in New York State or elsewhere ever been revoked, suspended or denied by any state, territory or governmental jurisdiction or foreign country, for any reason? ☐ No ☐ Yes If yes, you must submit all relevant documents, including the agency determination, if any.			
9. School Co-Director's Name		Gender	*Social Security Number
Telephone Number (area code + number)	Email Address (REQUIRED)		Department of State License Number or UID
9a. Has the SCHOOL CO-DIRECTOR ever been affiliated with or owned another proprietary school? ☐ No ☐ Yes If yes, please provide full details attached to this application, including any disallowances, fines, or any other disciplinary action against them or the school by any Local, State or Federal authorities.			
9b. Has the SCHOOL CO-DIRECTOR ever been convicted in this state or elsewhere of a crime, misdemeanor or felony? ☐ No ☐ Yes If yes, you must submit with this application a written explanation giving the place, court jurisdiction, nature of the offense, sentence and/or other disposition. You must submit a copy of the accusatory instrument (e.g., indictment, criminal information or complaint) and a Certificate of Disposition. If you possess or have received a Certificate of Relief from Disabilities, Certificate of Good Conduct or Executive Pardon, you must submit a copy with this application. Are there any criminal charges (misdemeanors or felonies) pending against you in any court in this state or elsewhere? ☐ No ☐ Yes If yes, you must submit a copy of the accusatory instrument (e.g., indictment, criminal information or complaint). Has any license, permit, commission, registration or application for a license, permit, commission, or registration held by you or a company in which you are or were a principal or employee in New York State or elsewhere ever been revoked, suspended or denied by any state, territory or governmental jurisdiction or foreign country, for any reason? ☐ No ☐ Yes If yes, you must submit all relevant documents, including the agency determination, if any.			
10. If a Partnership, complete the following for each Partner:			
Partner 1: Name	Gender	*Social Security Number	Date of Birth
Title	Department of State License Number or UID		
Home Address	Telephone Number (area code + number)		
10a. Has this individual ever been affiliated with or owned another proprietary school? ☐ No ☐ Yes If yes, please provide full details attached to this application, including any disallowances, fines, or any other disciplinary action against them or the school by any Local, State or Federal authorities.			
10b. Has this individual ever been convicted in this state or elsewhere of a crime, misdemeanor or felony? ☐ No ☐ Yes If yes, you must submit with this application a written explanation giving the place, court jurisdiction, nature of the offense, sentence and/or other disposition. You must submit a copy of the accusatory instrument (e.g., indictment, criminal information or complaint) and a Certificate of Disposition. If you possess or have received a Certificate of Relief from Disabilities, Certificate of Good Conduct or Executive Pardon, you must submit a copy with this application. Are there any criminal charges (misdemeanors or felonies) pending against this individual in any court in this state or elsewhere? ☐ No ☐ Yes If yes, you must submit a copy of the accusatory instrument (e.g., indictment, criminal information or complaint). Has any license, permit, commission, registration or application for a license, permit, commission, or registration held by you or a company in which you are or were a principal or employee in New York State or elsewhere ever been revoked, suspended or denied by any state, territory or governmental jurisdiction or foreign country, for any reason? ☐ No ☐ Yes If yes, you must submit all relevant documents, including the agency determination, if any.			
Partner 2: Name	Gender	*Social Security Number	Date of Birth
Title	Department of State License Number or UID		
Home Address	Telephone Number (area code + number)		

New York State Division of Criminal Justice Services
SECURITY GUARD PROGRAM – SECURITY GUARD TRAINING SCHOOL APPLICATION

SA

10a. Has this individual ever been affiliated with or owned another proprietary school? ☐ No ☐ Yes If yes , please provide full details attached to this application, including any disallowances, fines, or any other disciplinary action against them or the school by any Local, State or Federal authorities.			
10b. Has this individual ever been convicted in this state or elsewhere of a crime, misdemeanor or a felony? ☐ No ☐ Yes If yes , you must submit with this application a written explanation giving the place, court jurisdiction, nature of the offense, sentence and/or other disposition. You must submit a copy of the accusatory instrument (e.g., indictment, criminal information or complaint) and a Certificate of Disposition. If you possess or have received a Certificate of Relief from Disabilities, Certificate of Good Conduct or Executive Pardon, you must submit a copy with this application. Are there any criminal charges (misdemeanors or felonies) pending against this individual in any court in this state or elsewhere? ☐ No ☐ Yes If yes , you must submit a copy of the accusatory instrument (e.g., indictment, criminal information or complaint). Has any license, permit, commission, registration or application for a license, permit, commission, or registration held by you or a company in which you are or were a principal or employee in New York State or elsewhere ever been revoked, suspended or denied by any state, territory or governmental jurisdiction or foreign country, for any reason? ☐ No ☐ Yes If yes , you must submit all relevant documents, including the agency determination, if any.			
Partner 3: Name		Gender	*Social Security Number
Title		Department of State License Number or UID	
Home Address		Telephone Number (area code + number)	
10a. Has this individual ever been affiliated with or owned another proprietary school? ☐ No ☐ Yes If yes , please provide full details attached to this application, including any disallowances, fines, or any other disciplinary action against them or the school by any Local, State or Federal authorities.			
10b. Has this individual ever been convicted in this state or elsewhere of a crime, misdemeanor or felony? ☐ No ☐ Yes If yes , you must submit with this application a written explanation giving the place, court jurisdiction, nature of the offense, sentence and/or other disposition. You must submit a copy of the accusatory instrument (e.g., indictment, criminal information or complaint) and a Certificate of Disposition. If you possess or have received a Certificate of Relief from Disabilities, Certificate of Good Conduct or Executive Pardon, you must submit a copy with this application. Are there any criminal charges (misdemeanors or felonies) pending against this individual in any court in this state or elsewhere? ☐ No ☐ Yes If yes , you must submit a copy of the accusatory instrument (e.g., indictment, criminal information or complaint). Has any license, permit, commission, registration or application for a license, permit, commission, or registration held by you or a company in which you are or were a principal or employee in New York State or elsewhere ever been revoked, suspended or denied by any state, territory or governmental jurisdiction or foreign country, for any reason? ☐ No ☐ Yes If yes , you must submit all relevant documents, including the agency determination, if any.			
Partner 4: Name		Gender	*Social Security Number
Title		Department of State License Number or UID	
Home Address		Telephone Number (area code + number)	
10a. Has this individual ever been affiliated with or owned another proprietary school? ☐ No ☐ Yes If yes , please provide full details attached to this application, including any disallowances, fines, or any other disciplinary action against them or the school by any Local, State or Federal authorities.			
10b. Has this individual ever been convicted in this state or elsewhere of a crime, misdemeanor or a felony? ☐ No ☐ Yes If yes , you must submit with this application a written explanation giving the place, court jurisdiction, nature of the offense, sentence and/or other disposition. You must submit a copy of the accusatory instrument (e.g., indictment, criminal information or complaint) and a Certificate of Disposition. If you possess or have received a Certificate of Relief from Disabilities, Certificate of Good Conduct or Executive Pardon, you must submit a copy with this application. Are there any criminal charges (misdemeanors or felonies) pending against this individual in any court in this state or elsewhere? ☐ No ☐ Yes If yes , you must submit a copy of the accusatory instrument (e.g., indictment, criminal information or complaint). Has any license, permit, commission, registration or application for a license, permit, commission, or registration held by you or a company in which you are or were a principal or employee in New York State or elsewhere ever been revoked, suspended or denied by any state, territory or governmental jurisdiction or foreign country, for any reason? ☐ No ☐ Yes If yes , you must submit all relevant documents, including the agency determination, if any.			

New York State Division of Criminal Justice Services
SECURITY GUARD PROGRAM – SECURITY GUARD TRAINING SCHOOL APPLICATION

SA

If additional partners, attach additional sheets.

11. Audio/Visual Equipment to be used by school (i.e. PowerPoint, etc.)

12. Shipping Information

In order to provide mandated security guard training, approved security guard training schools and armed guard training schools must utilize Optical Mark Reader (OMR) forms for submission of training information to DCJS. These forms are provided by DCJS; however the school is responsible for the cost associated with shipping the forms. Provide a valid shipping account number with a company of your choosing.

Shipping Company

Account Number

13. Firearms Training Facility (to be completed by applicant applying for approval to conduct firearms training)

Name of Range

Type of Range

☐ Indoor

☐ Outdoor

Street Address

Room/Suite

City, State, Zip Code

County

Telephone Number (area code + number)

Facsimile Number (area code + number) (optional)

Contact Name

Contact Telephone Number (area code + number)

14. Certified Security Guard Instructors

GT= General Topics Instructor / **FA=** Firearms/Armed Security Guard Instructor (Check all that apply).

Instructor
Certifications

*Social Security Number

(Last Name, First Name, MI)

☐ FA ☐ GT

*Social Security Number

(Last Name, First Name, MI)

☐ FA ☐ GT

*Social Security Number

(Last Name, First Name, MI)

☐ FA ☐ GT

*Social Security Number

(Last Name, First Name, MI)

☐ FA ☐ GT

*Social Security Number

(Last Name, First Name, MI)

☐ FA ☐ GT

*Social Security Number

(Last Name, First Name, MI)

☐ FA ☐ GT

New York State Division of Criminal Justice Services
SECURITY GUARD PROGRAM – SECURITY GUARD TRAINING SCHOOL APPLICATION

SA

*Social Security Number	(Last Name, First Name, MI)	☐ FA ☐ GT
*Social Security Number	(Last Name, First Name, MI)	☐ FA ☐ GT
*Social Security Number	(Last Name, First Name, MI)	☐ FA ☐ GT
*Social Security Number	(Last Name, First Name, MI)	☐ FA ☐ GT

If additional space is required, attach a separate sheet.

15. Applicant Affirmation: This affidavit must be signed and sworn to by the Applicant before a Notary Public. I hereby affirm, under penalties of perjury, that the information provided in this application is true to the best of my knowledge and belief. I understand that any material misstatement may be deemed sufficient reason to deny approval, or may result in the suspension or revocation of the school approval, if issued. I hereby acknowledge that I have thoroughly read and understand General Business Law section 89-n and Parts 6027, 6028, and 6029 of Title 9 of the NYS Official Compilation of Codes, Rules and Regulations. I further understand that the School Director must attend the School Director Orientation Seminar required by Division of Criminal Justice Services (DCJS) and DCJS may ask for additional information/documentation.

Owner:

Notary Stamp

 Printed Name of Owner

 Owner's Signature

 Date

Sworn and subscribed before me
 this _____ day of _____ 20_____

 Notary Signature

I (school owner) give permission to the Division of Criminal Justice Services (DCJS) to include the school information on the listing of approved security guard training schools made available to the public. ☐ Yes ☐ No

School Director:

Notary Stamp

 Printed Name of School Director

 School Director Signature

 Date

Sworn and subscribed before me
 this _____ day of _____ 20_____

 Notary Signature

School Co-Director (if applicable):

Notary Stamp

 Printed Name of School Co-Director

 School Co-Director Signature

 Date

Sworn and subscribed before me
 this _____ day of _____ 20_____

 Notary Signature

New York State Division of Criminal Justice Services
SECURITY GUARD PROGRAM – SECURITY GUARD TRAINING SCHOOL APPLICATION

SA

DCJS Use Only

Application approved: Yes ☐ No ☐ Date: _____

Approved by (printed name): _____ Signature: _____ Date: _____

Comments:

This form must be submitted to the Division of Criminal Justice Services (DCJS) to receive approval for each school training site. The form provides information on the facilities to determine if they are satisfactory for the proper conduct of mandated security guard training. The facilities must be properly equipped and meet local fire and building standards. At least sixteen square feet must be allotted per student. The Division will identify the number of students allowable for each individual training session based on the square footage of the classroom and equipment etc., located in the space. The number of students allowable in any one training session cannot exceed 35. Training sites used for non firearms security guard training must be handicap accessible. A Certificate of Occupancy; fire authority approval; a floor plan; and digital photographs of the exterior of the premises, building handicap accessibility elements, and interior rooms identified on the floor plan must be submitted with this form. The Division reserves the right to inspect the training site prior to approval.

Certificate of Occupancy

The training site must be approved for use as a school by the municipality in which the site is located. A copy of a valid Certificate of Occupancy must be included with this form. The training site address must be the same as the address listed on the Certificate of Occupancy.

A Certificate of Occupancy (CO) is issued by local municipalities to verify that local building codes have been met and the building is suitable for occupancy. It further states the purpose for which the quarters are to be used (i.e., commercial, residential, school, etc.)

To obtain a copy of a CO in NYC, visit the Department of Buildings' Customer Service Counter in your borough office or log on to the Building Information System at <http://nyc.gov/bis>. If a building was constructed before 1938 and there has been no change in use or additions to the property, it may not have a CO. To obtain proof of the legal use of a building that does not have a CO, you must obtain a "Letter of No Objection" from the Department of Buildings' borough office where the property is located.

*A Certificate of Occupancy is required for all structures; however, certain enterprises may be waived from the requirement that the CO specifically approves the site for school use.

**Submission of a Certificate of Occupancy may be waived for governmental agencies, municipalities and public or private educational institutions in NY or any other jurisdiction.

***If a municipality does not issue Certificates of Occupancy for existing structures, you must submit a letter from the municipality to that effect.

Zoning Compliance Letter

Submit proof that the site to be used to conduct training is legal and is permitted at that location.

*A Zoning Compliance Letter is required for all training sites; however, certain enterprises may be waived from the requirement that the Zoning Compliance Letter specifically approve the site for school use.

**Submission of a Zoning Compliance Letter may be waived for governmental agencies or municipalities and public or private secondary or collegiate-level educational institutions in NY or any other jurisdiction.

Fire Approval

The premises in which mandated security guard training courses will be conducted must be approved for occupancy by the fire authority of the municipality or county in which the site is located. The approval must have been granted during the past three (3) years. The address listed on the fire authority approval must be the same as the address listed in Number 4 (Training Site) of the application. In some circumstances the applicant may not yet have rented the premises. If this is the case, the approval may be missing from the application packet. However, the premises must be rented upon notice to you by DCJS that your approval is nearing completion and Fire Authority Approval must be provided for final approval of the application.

Handicap Accessibility

Training sites used for non firearms security guard training must be handicap accessible. Title III of the American with Disabilities Act (effective January 26, 1992), requires private businesses to be accessible to persons with disabilities. Provide photographs (digital or hard copy) of the handicap accessibility elements of the building.



New York State Division of Criminal Justice Services
SECURITY GUARD PROGRAM – TRAINING SITE APPROVAL REQUEST

Floor Plans

Floor plans must be drawn to scale of at least ¼" equaling 1". DCJS reserves the right to request a different scale if necessary. The scale must be indicated on the plans. Each room must be assigned a number and the proposed use of the room and square footage must be listed below (e.g., classroom, bathroom, office, etc.). The floor plans must show:

1. Dimensions of each room or unit of space;
2. Entrances and exits, stairways, corridors, fire escapes;
3. Windows;
4. Student work stations (desks, chairs), furniture, blackboard, white board, audio visual equipment, etc.; and
5. Utilities – heating and air conditioning, and lighting.

*Submission of a floor plan may be waived for governmental agencies or municipalities and public or private secondary or collegiate-level educational institutions in NY or any other jurisdiction.

Photographs

For the training site, digital photographs of the exterior of the premises, building handicap accessibility elements and interior rooms identified on the floor plan must be submitted. Digital photographs must be on a CD/DVD disk or USB flash drive and submitted with the floor plan. For the firearms facility, provide digital photographs of the indoor range (if applicable), the exterior and interior of the classroom(s) and bathroom(s). A floor plan is not required for the firearms facility classroom.

NEW YORK STATE DIVISION OF CRIMINAL JUSTICE SERVICES

School Name:	School Identification No:
School Address:	Room/Suite:
City, State, Zip Code:	County:
Telephone Number (area code + number):	
School Owner Name(s):	
School Director Name:	

Training Site Address (if different than above):	
City, State, Zip Code:	County
Training Site Floor Level (e.g., Street level, 2 nd floor, 3 rd floor, etc.):	Is the site handicap accessible: Yes ☐ No ☐

Audio Visual Equipment:

Firearms Facility Name of Range:	
Range Street Address:	County:
City, State, Zip Code:	Range Telephone Number (area code + number):
Range Contact:	Contact Telephone Number (area code + number):
Number of Lanes:	Indoor ☐ Outdoor ☐
Entity that Approved Range:	Facility meets applicable lead safety standards. ☐
Identify safety features of the range (bullet resistant glass, etc.):	

Room Specific Information		
Room Number:	Proposed use of room:	Floor Space in Square Feet:
Room Number:	Proposed use of room:	Floor Space in Square Feet:
Room Number:	Proposed use of room:	Floor Space in Square Feet:
Room Number:	Proposed use of room:	Floor Space in Square Feet:
Room Number:	Proposed use of room:	Floor Space in Square Feet:

_____ Printed Name of Requester (School Owner or School Director only)	_____ Title (School Owner or School Director)
_____ Signature of Requestor	_____ Date

Submit Completed Form to: NYS Division of Criminal Justice Services, Office of Public Safety, Security Guard Program, 80 S. Swan Street, Albany, NY 12210
Direct questions to the Security Guard Program at (518) 457-4135.



New York State Division of Criminal Justice Services
SECURITY GUARD PROGRAM – TRAINING SITE APPROVAL REQUEST

DCJS Use Only

Floor plan submitted: Yes ☐ No ☐ Date: _____ Digital photographs submitted: Yes ☐ No ☐ Date: _____

Certificate of Occupancy submitted: Yes ☐ No ☐ Date: _____ Zoning Letter Submitted: Yes ☐ No ☐ Date: _____

Fire Approval submitted: Yes ☐ No ☐ Date: _____

Training site handicap accessible (required for sites to be used for non firearms security guard training): Yes ☐ No ☐
Date: _____

Number of students allowable per training session based on square footage and equipment etc. located in the space: _____

Training site approved: Yes ☐ No ☐ Date: _____

Approved by (printed name): _____ Signature: _____ Date: _____

Comments:



THIS FORM IS USED TO APPLY FOR RENEWAL OF A SECURITY GUARD TRAINING SCHOOL. FORMS PRESENTED FOR FILING MUST CONTAIN ORIGINAL SIGNATURES. THE BLANK FORM MAY BE DUPLICATED, HOWEVER PHOTOCOPIES OF COMPLETED FORMS, OR FORMS WITH PHOTOCOPIED SIGNATURES WILL NOT BE ACCEPTED. TYPE ALL INFORMATION. OMISSIONS OR LACK OF INFORMATION WILL STOP THE REVIEW PROCESS. THE SCHOOL DIRECTOR MAY BE REQUIRED TO ATTEND AN ORIENTATION SEMINAR IN ALBANY.

Security Guard Training Schools must be approved by the Division of Criminal Justice Services (DCJS), pursuant to Title 9 of the Official Compilation of Codes, Rules, and Regulations of New York State, Part 6028. **Security Guard Training Schools are approved to conduct either mandated non-firearms security guard training, mandated security guard firearms training, or both.**

The process for applying for renewal of a security guard training school consists of the three types of documentation listed below. Each section is discussed in detail in the following material.

- I. Application
- II. Forms and Documentation
- III. School Prepared Forms

DCJS reserves the right to require further documentation as necessary to properly identify school owners and school directors, verify contact information and determine whether the school location meets DCJS standards for classroom instruction.

A non-refundable fee of \$500 must be submitted with the Security Guard School Renewal Application. Payment must be in the form of a money order, bank certified check, or corporate check and made payable to the NYS Division of Criminal Justice Services (DCJS).

*Pursuant to the New York State Personal Privacy Protection Law, DCJS is authorized to collect personal identifying information as part of a public safety agency record. Personal identifying information on this form shall not be revealed, released, transferred, disseminated, or otherwise communicated orally, in writing, or by electronic means other than to the applicant. Disclosure of personal identifying information is voluntary. Refusal to provide personal identifying information shall not result in the denial of any right, benefit, or privilege.

The applicant will receive the school's approval, or a letter detailing the reason for denial of the application within 120 days of receipt of a complete application. A complete application must contain all information and supporting documentation as outlined below. All of the information requested must be submitted, or the application will be denied.

SECTION I: SCHOOL APPLICATION INFORMATION

TYPE OF TRAINING FOR WHICH APPLICATION IS BEING MADE: Check the type of security guard training the school is applying for. If applying to conduct both types of training, check both boxes.

1. **School Name** – This is the name your school will be utilizing and which will appear on your approval certificate issued by DCJS. If the name of the school is other than your own legal name, the name must be registered. Before filing your Business Certificate as a Sole Proprietor or Partnership, the County Clerk's Office will make a determination of name availability. The Department of State will make a determination on name availability for a corporation, foreign corporation, limited liability company, limited liability partnership, and a limited partnership.
2. **Federal Tax Identification Number or Employer Identification Number** – The school owner (applicant) 9-digit number from the Internal Revenue Service that identifies the school as a business entity.
3. **School Mailing Address** - Provide the mailing address of the school.
4. **School Training Site Address** – This is the address where mandated security guard training courses will be conducted. The training site must have a local certificate of occupancy approving its use for "school purposes" as well as approval from the fire authorities in the jurisdiction where the site is located. DCJS requires that 16 square feet be allotted per student. A determination of the number of students allowed in each training session will be made by DCJS based on the square footage of the classroom and equipment etc. located in the space. You may leave this blank if you have not yet rented the training site. However, the site must be rented upon notice to you by DCJS that your approval is nearing completion and a certificate of occupancy must be provided for final approval. For identification purposes you must provide DCJS with the city where the proposed school is located. **You must complete the Request for Approval of a Training Site for this address.**
5. **Handicap Accessibility** - The training site utilized for mandated non-firearms security guard training must be handicap accessible. Title III of the American with Disabilities Act (effective January 26, 1992), requires private businesses to be accessible to persons with disabilities. The applicant must provide digital photographs of the handicap accessibility elements of the building.
6. **Type of Owner of School** – Proprietorship, partnership, corporation, Not for Profit Corporation, public or private collegiate educational institution, public or private educational institution, governmental agency/entity, or other.



7. **Name of School Owner or Corporation (Applicant), contact and other required information** – If corporation, this should be exactly as it appears on your Certificate of Incorporation. Enter contact information. If sole owner (proprietor), enter your gender, date of birth, and *social security number. The school owner must meet minimum requirements pursuant to 9 NYCRR Part 6028 to include being an officer, member, or principal currently licensed by the Department of State as a private investigator; watch, guard or patrol agency; or armored car carrier agency; or maintain a valid security guard registration card issued by the Department of State; or maintain a valid armored car guard registration card issued by the Department of State.
- 7a. **Affiliation with another school** – The school owner, whose name appears on the application, must answer whether they have ever been affiliated with or owned another proprietary school. If yes, full details of such association, including any fiscal disallowances, fine or penalty, or any other disciplinary action against them or the school by any Local, State or Federal authorities must be provided on a separate sheet.
- 7b. **Disclosure** – The school owner whose name appears on the application must state whether they:
- Have ever been convicted in this state or elsewhere of a crime or offense that is a misdemeanor or a felony. **If yes**, a written explanation giving the place, sentencing court, nature of the offense, sentence and/or other disposition, a copy of the accusatory instrument (e.g. indictment, criminal information, or complaint) and a Certificate of Disposition must be submitted with the application. A Certificate of Relief from Disabilities, Certificate of Good Conduct or Executive Pardon, if applicable, must be submitted with the application.
 - Have any criminal charges (misdemeanors or felonies) pending against them. **If yes**, a copy of the accusatory instrument (e.g. indictment, criminal information, or complaint) must be submitted with the application.
 - Has any license, permit, commission, registration, approval, or application for a license, permit, commission, approval, or registration held by them or a company in which they are or were a principal or employee in New York State or elsewhere ever been revoked, suspended, or denied by any state, territory, or governmental jurisdiction or foreign country, for any reason. **If yes**, submit any relevant documents, including the agency determination.
8. **Name of School Director, contact and other required information** – Enter the name, contact information, gender and social security number of the of the school director. The school director must meet minimum requirements pursuant to 9 NYCRR Part 6028 to include being an officer, member, or principal currently licensed by the Department of State as a private investigator; watch, guard or patrol agency; or armored car carrier agency; or maintain a valid security guard registration card issued by the Department of State; or maintain a valid armored car guard registration card issued by the Department of State.
- 8a. **Affiliation with another school** – The school director, whose name appears on the application, must answer whether they have ever been affiliated with or owned another proprietary school. If yes, full details of such association, including any fiscal disallowances, fine or penalty, or any other disciplinary action against them or the school by any Local, State or Federal authorities must be provided on a separate sheet.
- 8b. **Disclosure** – The school director whose name appears on the application must state whether they:
- Have ever been convicted in this state or elsewhere of a crime or offense that is a misdemeanor or a felony. **If yes**, a written explanation giving the place, court jurisdiction, nature of the offense, sentence and/or other disposition, a copy of the accusatory instrument (e.g. indictment, criminal information, or complaint) and a Certificate of Disposition must be submitted with the application. A Certificate of Relief from Disabilities, Certificate of Good Conduct or Executive Pardon, if applicable, must be submitted with the application.
 - Have any criminal charges (misdemeanors or felonies) pending against them. **If yes**, a copy of the accusatory instrument (e.g. indictment, criminal information, or complaint) must be submitted with the application.
 - Has any license, permit, commission, registration, approval, or application for a license, permit, commission, approval, or registration held by them or a company in which they are or were a principal or employee in New York State or elsewhere ever been revoked, suspended, or denied by any state, territory, or governmental jurisdiction or foreign country, for any reason. **If yes**, submit any relevant documents, including the agency determination.
9. **Name of School Co-Director (if applicable), contact and other required information** – Enter the name, contact information, gender and social security number of the school co-director. There is no requirement that an applicant have a co-director. The school co-director must meet minimum requirements pursuant to 9 NYCRR Part 6028 to include being an officer, member, or principal currently licensed by the Department of State as a private investigator; watch, guard or patrol agency; or armored car carrier agency; or maintain a valid security guard registration card issued by the Department of State; or maintain a valid armored car guard registration card issued by the Department of State.
- 9a. **Affiliation with another school** – The school co-director, whose name appears on the application, must answer whether they have ever been affiliated with or owned another proprietary school. If yes, full details of such



association, including any fiscal disallowances, fine or penalty, or any other disciplinary action against them or the school by any Local, State or Federal authorities must be provided on a separate sheet.

9b. **Disclosure** – The school co-director whose name appears on the application must state whether they:

- Have ever been convicted in this state or elsewhere of a crime or offense that is a misdemeanor or a felony. **If yes**, a written explanation giving the place, court jurisdiction, nature of the offense, sentence and/or other disposition, a copy of the accusatory instrument (e.g. indictment, criminal information, or complaint) and a Certificate of Disposition must be submitted with the application. A Certificate of Relief from Disabilities, Certificate of Good Conduct or Executive Pardon, if applicable, must be submitted with the application.
- Have any criminal charges (misdemeanors or felonies) pending against them. **If yes**, a copy of the accusatory instrument (e.g. indictment, criminal information, or complaint) must be submitted with the application.
- Has any license, permit, commission, registration, approval, or application for a license, permit, commission, approval, or registration held by them or a company in which they are or were a principal or employee in New York State or elsewhere ever been revoked, suspended, or denied by any state, territory, or governmental jurisdiction or foreign country, for any reason. **If yes**, submit any relevant documents, including the agency determination.

10. **Partners** – If the ownership is a partnership, enter the name of the partner(s), social security number, date of birth, and contact information. Indicate whether they have ever been affiliated with or owned another proprietary school. If yes, provide full details attached to this application, including any disallowances, fines, denial of license or approval, or any disciplinary action against them or the school by any local, state, or Federal authorities.

10a. **Affiliation with another school** – The applicant must answer for each partner whose name appears on the application, whether they have ever been affiliated with or owned another proprietary school. If yes, full details of such association, including any fiscal disallowances, fine or penalty, or any other disciplinary action against them or the school by any Local, State or Federal authorities must be provided on a separate sheet.

10b. **Disclosure** – The applicant must answer for each partner whose name appears on the application, whether they:

- Have ever been convicted in this state or elsewhere of a crime or offense that is a misdemeanor or a felony. **If yes**, a written explanation giving the place, court jurisdiction, nature of the offense, sentence and/or other disposition, a copy of the accusatory instrument (e.g. indictment, criminal information, or complaint) and a Certificate of Disposition must be submitted with the application. A Certificate of Relief from Disabilities, Certificate of Good Conduct or Executive Pardon, if applicable, must be submitted with the application.
- Have any criminal charges (misdemeanors or felonies) pending against them. **If yes**, a copy of the accusatory instrument (e.g. indictment, criminal information, or complaint) must be submitted with the application.
- Have had any license, permit, commission, registration, approval, or application for a license, permit, commission, approval, or registration held by them or a company in which they are or were a principal or employee in New York State or elsewhere ever revoked, suspended, or denied by any state, territory, or governmental jurisdiction or foreign country, for any reason. **If yes**, submit any relevant documents, including the agency determination.

11. **Audio/Visual Equipment** – Identify the type of audio/visual equipment to be used by the school.

12. **Shipping Information** - In order to provide mandated security guard training, security guard training schools must utilize Optical Mark Reader (OMR) forms for submission of training information to DCJS. These forms are provided by DCJS; however the school is responsible for the cost associated with the shipment of the forms. Enter the name and account number of the shipping company to be used for shipment of Optical Mark Reader forms.

13. **Firearms Training Facility** – To be completed by applicant applying for approval to conduct firearms training. Enter the name of the range and street address (do not enter a post office box), city, state, zip code, county and business telephone number, and type of range (outdoor or indoor facility). Enter the name and telephone number of the contact person for the firearms facility. **You must complete the Request for Approval of Training Site form for this address.** Refer to Section II for additional information.

14. **Certified Security Guard Instructors** - Enter the names of **ALL** DCJS certified security guard instructor(s) or armed security guard instructor(s) to be utilized by your school. All instructors must possess a valid certification. Instructor certifications are valid for a period of five years, at which time the instructor must apply for renewal. Application to conduct firearms training requires a minimum of one DCJS certified armed security guard instructor. Application to conduct non-firearms security guard training requires a minimum of one DCJS certified security guard instructor.



Enter the social security number, name of instructor as it appears on the certification letter, and type of certification. Check all that apply, GT for General Topics Instructor, FA for Firearms/Armed Security Guard Instructor.

15. **Intent to Provide Security Guard Training** – DCJS provides complete lesson plans for the 8 Hour Pre-Assignment Training Course for Security Guards, the 16 Hour General On-The-Job Training Course for Security Guards, the 47 Hour Firearms Course for Armed Security Guards, and the 8 Hour Annual In-Service Course for Armed Security Guards. Check the boxes for the courses for which the school is using the complete lessons provided by DCJS.

Check the appropriate boxes If your school has developed its own lesson plans for the 8 Hour Pre-Assignment Training Course for Security Guards and/or the 16 Hour On-The-Job Training Course for Security Guards in accordance with Part 6027 of the Official Compilation of Codes, Rules and Regulations of the State of New York (9 NYCRR). **Submit course outline(s) with topics, objectives, duration for each module and a bank of 50 examination questions with the School Renewal Application for review and approval.**

*****Eight Hour Annual In-Service Course for Security Guards**

If an approved security guard training school plans to, or is conducting the Eight Hour Annual In-Service Course for Security Guards, the school is required to develop lesson plans utilizing topics outlined in 9 NYCRR Part 6027. **The school must submit a course outline with topics, objectives, and duration for each module of instruction with the School Renewal Application.**

16. **Applicant Affirmation** – This is an affirmation to the accuracy of information provided on the application, an acknowledgment related to General Business Law section 89-n and the NYS Official Compilation of Codes, Rules and Regulations, and that the school director may be required to attend an orientation seminar. This must be signed and sworn to by the applicant, school director, and school co-director (if applicable) before a notary public.

SECTION II: FORMS AND DOCUMENTATION

1. **Type of Ownership** – Applicants must provide supporting documents with application for type of ownership. If the type of ownership checked on the application is “Other”, provide applicable documentation.
- a. Sole Proprietorship – Provide consent to do business from county clerk
 - b. Partnership – Provide copy of partnership agreement
 - c. Corporation – Provide Certificate of Incorporation and if applicable, certificate of assumed name
2. **Certificate of Occupancy** – Issued by the municipality in which the training site is located to verify that the training site address is approved for use as a school. A valid Certificate of Occupancy must be included with the application. The address on the certificate must be the same address listed in Number 4 (Training Site) on the application. In some circumstances the applicant may not yet have rented the training site. If this is the case, the Certificate of Occupancy may be missing from the application packet. However, the training site must be rented upon notice to you by DCJS that your approval is nearing completion and a Certificate must be provided for final approval.

A Certificate of Occupancy (CO) is issued by local municipalities to verify that local building codes have been met and the building is suitable for occupancy. It further states the purpose for which the quarters are to be used (i.e., commercial, residential, school, etc.)

To obtain a copy of a CO in NYC, visit the Department of Buildings' Customer Service Counter in your borough office or log on to the Building Information System at <http://nyc.gov/bis>. If a building was constructed before 1938 and there has been no change in use or additions to the property, it may not have a CO. To obtain proof of the legal use of a building that does not have a CO, you must obtain a “Letter of No Objection” from the Department of Buildings' borough office where the property is located. **Applicant must submit a “Letter of No Objection” should the building not have a CO.**

*A Certificate of Occupancy is required for all training sites; however, certain enterprises may be waived from the requirement that the CO specifically approve the site for school use.

**Submission of a Certificate of Occupancy may be waived for governmental agencies or municipalities and public or private secondary or collegiate-level educational institutions in NY or any other jurisdiction.

***If a municipality does not issue COs for existing structures, you must submit a letter from the municipality to that effect.

3. **Zoning Compliance Letter** – Submit proof that the site to be used to conduct training conforms with local zoning laws and regulations. The address in the letter must be the same address listed in Number 4 (Training Site) on the application.



*A Zoning Compliance Letter is required for all training sites; however, certain enterprises may be waived from the requirement that the Zoning Compliance Letter specifically approve the site for school use.

**Submission of a Zoning Compliance Letter may be waived for governmental agencies or municipalities and public or private secondary or collegiate-level educational institutions in NY or any other jurisdiction.

4. **Proof of Insurance for the conduct of firearms training** – An applicant applying for approval to conduct firearms training which is self-insured must submit a Certificate of Insurance evidencing comprehensive general liability coverage from an insurance agency licensed to do business in New York State or procured by a duly licensed excess line broker pursuant to §2118 of the NYS Insurance Law in the minimum amount of \$100,000 per occurrence and \$300,000 in the aggregate which amount shall be available for the payment of claims. The applicant must provide a copy of the Certificate of Insurance. In some circumstances the applicant may not yet have purchased liability insurance. If this is the case, the Certificate of Insurance may be missing from the application packet. However, it must be submitted upon notice to you by DCJS that your approval is nearing completion and the Certificate must be provided for final approval of the application.
5. **Fire Authority Approval** - The premises in which mandated security guard training courses will be conducted must be approved for occupancy by the fire authority of the municipality or county in which the site is located. The approval must have been granted during the past three (3) years. The address listed on the fire authority approval must be the same as the address listed in Number 4 (Training Site) of the application. In some circumstances the applicant may not yet have rented the premises. If this is the case, the approval may be missing from the application packet. However, the premises must be rented upon notice to you by DCJS that your approval is nearing completion and Fire Authority Approval must be provided for final approval of the application.
6. **Request for Approval of a Training Site** – A Request for Approval of Training Site form must be completed for the address listed in Number 4 (Training Site) of the application. If the school has more than one training site, the form must be completed for each site. A floor plan must be submitted for the address listed in Number 4 (Training Site) of the application and for any additional training sites. The plan must be drawn to scale of at least ¼" equaling 1". All standard architectural features such as windows, doors, and permanent fixtures should be clearly labeled. The room number, all dimensions, and the use of each room or space must also be clearly labeled. Digital photographs of the exterior of the premises, building handicap accessibility elements and interior rooms identified on the floor plan must be submitted with the floor plan. Digital photos must be submitted on a CD/DVD disk or USB flash drive. In some instances the applicant may have not rented the premises. If this is the case, the photographs and floor plan may be missing from the application packet. However, the premises must be rented upon notice to you by DCJS that your approval is nearing completion and the photographs and floor plan must be provided for final approval of the application. **DCJS reserves the right to inspect the training site prior to approval.**

*Submission of the floor plan may be waived for governmental agencies or municipalities and public or private secondary or collegiate-level educational institutions in NY or any other jurisdiction.

SECTION III: SCHOOL PREPARED FORMS

Approved security guard schools are required to have the following forms. Forms may be in a printer's proof format until approval to print the forms is received from DCJS.

1. Printed catalogue or booklet of mandated security guard training courses to be offered by the school. The catalogue must include a description of each course, when the courses are to be completed (i.e. 16 Hour On-the Job Training Course must be completed within 90 days of employment), school attendance policy (policy must be compliant with 9 NYCRR Part 6027) and the school's refund policy;
2. Printed enrollment agreement. The enrollment agreement must include a refund policy statement. Agents/employees of the school that enroll students must be identified on the enrollment agreement by printed name and signature; and
3. Payment Receipt Form - for issuance to students for verification of payment. The form must identify how payment was made (e.g. cash, check, credit card etc.) and the school name must appear on the receipt form.

MAIL APPLICATION, DOCUMENTATION AND PAYMENT TO:

Kimberly Szady, Director of Finance
NYS Division of Criminal Justice Services
Office of Financial Services
Alfred E. Smith Office Building,
80 South Swan Street
Albany, NY 12210

***Do Not Mail Cash, Personal Checks, or Credit Cards**



New York State Division of Criminal Justice Services
SECURITY GUARD PROGRAM – SECURITY GUARD TRAINING SCHOOL RENEWAL APPLICATION

RA

SECTION I: TRAINING SCHOOL INFORMATION

TYPE OF TRAINING: ☐ **SECURITY GUARD TRAINING (NON-FIREARMS)** ☐ **FIREARMS SECURITY GUARD TRAINING**

1. School Name		2. Federal Tax ID Number/Employer ID Number		School Code	
3. School Mailing Address				Room/Suite	
City, State, Zip Code				County	
4. Training Site Street Address (if different from school mailing address)				Training Site Room/Suite	
Training Site City, State, Zip Code				Training Site County	
Telephone Number (area code + number)			Facsimile Number (area code + number) (optional)		
5. Handicap Accessible Yes ☐ No ☐		6. Type of Ownership of School (check one) Proprietorship ☐ Partnership ☐ Corporation ☐ Not for Profit Corporation ☐ public or private collegiate education institution ☐ public or private education institution ☐ governmental agency/entity ☐ Other (provide type) ☐ _____			
7. School Owner or Corporation Name and Dept. of State License Number or UID			Owner's Name and Title		
Street Address			City, State, Zip Code		Telephone Number (area code + number)
If sole owner (proprietor) of school provide the following:					
Gender		Date of Birth		*Social Security Number	
				Email Address	
7a. Has the SCHOOL OWNER ever been affiliated with or owned another proprietary school? ☐ No ☐ Yes If yes , please provide full details attached to this application, including any disallowances, fines, or any other disciplinary action against them or the school by any Local, State or Federal authorities.					
7b. Has the SCHOOL OWNER ever been convicted in this state or elsewhere of a crime, misdemeanor or a felony? ☐ No ☐ Yes If yes , you must submit with this application a written explanation giving the place, court jurisdiction, nature of the offense, sentence and/or other disposition. You must submit a copy of the accusatory instrument (e.g., indictment, criminal information or complaint) and a Certificate of Disposition. If you possess or have received a Certificate of Relief from Disabilities, Certificate of Good Conduct or Executive Pardon, you must submit a copy with this application. Are there any criminal charges (misdemeanors or felonies) pending against you in any court in this state or elsewhere? ☐ No ☐ Yes If yes , you must submit a copy of the accusatory instrument (e.g., indictment, criminal information or complaint). Has any license, permit, commission, registration or application for a license, permit, commission, or registration held by you or a company in which you are or were a principal or employee in New York State or elsewhere ever been revoked, suspended or denied by any state, territory or governmental jurisdiction or foreign country, for any reason? ☐ No ☐ Yes If yes , you must submit all relevant documents, including the agency determination, if any.					
8. School Director's Name			Gender		*Social Security Number
Telephone Number (area code + number)		Email Address (REQUIRED)		Department of State License Number or UID	
8a. Has the SCHOOL DIRECTOR ever been affiliated with or owned another proprietary school? ☐ No ☐ Yes If yes , please provide full details attached to this application, including any disallowances, fines, or any other disciplinary action against them or the school by any Local, State or Federal authorities.					
8b. Has the SCHOOL DIRECTOR ever been convicted in this state or elsewhere of a crime, misdemeanor or felony? ☐ No ☐ Yes If yes , you must submit with this application a written explanation giving the place, court jurisdiction, nature of the offense, sentence and/or other disposition. You must submit a copy of the accusatory instrument (e.g., indictment, criminal information or complaint) and a Certificate of Disposition. If you possess or have received a Certificate of Relief from Disabilities, Certificate of Good Conduct or Executive Pardon, you must submit a copy with this application. Are there any criminal charges (misdemeanors or felonies) pending against you in any court in this state or elsewhere? ☐ No ☐ Yes If yes , you must submit a copy of the accusatory instrument (e.g., indictment, criminal information or complaint). Has any license, permit, commission, registration or application for a license, permit, commission, or registration held by you or a company in which you are or were a principal or employee in New York State or elsewhere ever been revoked, suspended or denied by any state, territory or governmental jurisdiction or foreign country, for any reason? ☐ No ☐ Yes If yes , you must submit all relevant documents, including the agency determination, if any.					

New York State Division of Criminal Justice Services
SECURITY GUARD PROGRAM – SECURITY GUARD TRAINING SCHOOL RENEWAL APPLICATION

RA

9. School Co-Director's Name		Gender	*Social Security Number	
Telephone Number (area code + number)		Email Address (REQUIRED)		Department of State License Number or UID

9a. Has the **SCHOOL CO-DIRECTOR** ever been affiliated with or owned another proprietary school? ☐ No ☐ Yes

If **yes**, please provide full details attached to this application, including any disallowances, fines, or any other disciplinary action against them or the school by any Local, State or Federal authorities.

9b. Has the **SCHOOL CO-DIRECTOR** ever been convicted in this state or elsewhere of a crime, misdemeanor or felony? ☐ No ☐ Yes

If **yes**, you must submit with this application a written explanation giving the place, court jurisdiction, nature of the offense, sentence and/or other disposition. You must submit a copy of the accusatory instrument (e.g., indictment, criminal information or complaint) and a Certificate of Disposition. If you possess or have received a Certificate of Relief from Disabilities, Certificate of Good Conduct or Executive Pardon, you must submit a copy with this application.

Are there any criminal charges (misdemeanors or felonies) pending against you in any court in this state or elsewhere? ☐ No ☐ Yes

If **yes**, you must submit a copy of the accusatory instrument (e.g., indictment, criminal information or complaint).

Has any license, permit, commission, registration or application for a license, permit, commission, or registration held by you or a company in which you are or were a principal or employee in New York State or elsewhere ever been revoked, suspended or denied by any state, territory or governmental jurisdiction or foreign country, for any reason? ☐ No ☐ Yes

If **yes**, you must submit all relevant documents, including the agency determination, if any.

10. If a Partnership, complete the following for each Partner:

Partner 1: Name		Gender	*Social Security Number	Date of Birth
Title		Department of State License Number or UID		
Home Address		Telephone Number (area code + number)		

10a. Has this individual ever been affiliated with or owned another proprietary school? ☐ No ☐ Yes

If **yes**, please provide full details attached to this application, including any disallowances, fines, or any other disciplinary action against them or the school by any Local, State or Federal authorities.

10b. Has this individual ever been convicted in this state or elsewhere of a crime, misdemeanor or felony? ☐ No ☐ Yes

If **yes**, you must submit with this application a written explanation giving the place, court jurisdiction, nature of the offense, sentence and/or other disposition. You must submit a copy of the accusatory instrument (e.g., indictment, criminal information or complaint) and a Certificate of Disposition. If you possess or have received a Certificate of Relief from Disabilities, Certificate of Good Conduct or Executive Pardon, you must submit a copy with this application.

Are there any criminal charges (misdemeanors or felonies) pending against this individual in any court in this state or elsewhere? ☐ No ☐ Yes

If **yes**, you must submit a copy of the accusatory instrument (e.g., indictment, criminal information or complaint).

Has any license, permit, commission, registration or application for a license, permit, commission, or registration held by you or a company in which you are or were a principal or employee in New York State or elsewhere ever been revoked, suspended or denied by any state, territory or governmental jurisdiction or foreign country, for any reason? ☐ No ☐ Yes

If **yes**, you must submit all relevant documents, including the agency determination, if any.

Partner 2: Name		Gender	*Social Security Number	Date of Birth
Title		Department of State License Number or UID		
Home Address		Telephone Number (area code + number)		

10a. Has this individual ever been affiliated with or owned another proprietary school? ☐ No ☐ Yes

If **yes**, please provide full details attached to this application, including any disallowances, fines, or any other disciplinary action against them or the school by any Local, State or Federal authorities.

10b. Has this individual ever been convicted in this state or elsewhere of a crime, misdemeanor or a felony? ☐ No ☐ Yes

If **yes**, you must submit with this application a written explanation giving the place, court jurisdiction, nature of the offense, sentence and/or other disposition. You must submit a copy of the accusatory instrument (e.g., indictment, criminal information or complaint) and a Certificate of Disposition. If you possess or have received a Certificate of Relief from Disabilities, Certificate of Good Conduct or Executive Pardon, you must submit a copy with this application.

Are there any criminal charges (misdemeanors or felonies) pending against this individual in any court in this state or elsewhere? ☐ No ☐ Yes

If **yes**, you must submit a copy of the accusatory instrument (e.g., indictment, criminal information or complaint).

Has any license, permit, commission, registration or application for a license, permit, commission, or registration held by you or a company in which you are or were a principal or employee in New York State or elsewhere ever been revoked, suspended or denied by any state, territory or governmental jurisdiction or foreign country, for any reason? ☐ No ☐ Yes

If **yes**, you must submit all relevant documents, including the agency determination, if any.

New York State Division of Criminal Justice Services
SECURITY GUARD PROGRAM – SECURITY GUARD TRAINING SCHOOL RENEWAL APPLICATION

RA

Partner 3: Name	Gender	*Social Security Number	Date of Birth
Title	Department of State License Number or UID		
Home Address	Telephone Number (area code + number)		
10a. Has this individual ever been affiliated with or owned another proprietary school? ☐ No ☐ Yes If yes, please provide full details attached to this application, including any disallowances, fines, or any other disciplinary action against them or the school by any Local, State or Federal authorities.			
10b. Has this individual ever been convicted in this state or elsewhere of a crime, misdemeanor or felony? ☐ No ☐ Yes If yes, you must submit with this application a written explanation giving the place, court jurisdiction, nature of the offense, sentence and/or other disposition. You must submit a copy of the accusatory instrument (e.g., indictment, criminal information or complaint) and a Certificate of Disposition. If you possess or have received a Certificate of Relief from Disabilities, Certificate of Good Conduct or Executive Pardon, you must submit a copy with this application. Are there any criminal charges (misdemeanors or felonies) pending against this individual in any court in this state or elsewhere? ☐ No ☐ Yes If yes, you must submit a copy of the accusatory instrument (e.g., indictment, criminal information or complaint). Has any license, permit, commission, registration or application for a license, permit, commission, or registration held by you or a company in which you are or were a principal or employee in New York State or elsewhere ever been revoked, suspended or denied by any state, territory or governmental jurisdiction or foreign country, for any reason? ☐ No ☐ Yes If yes, you must submit all relevant documents, including the agency determination, if any.			
Partner 4: Name	Gender	*Social Security Number	Date of Birth
Title	Department of State License Number or UID		
Home Address	Telephone Number (area code + number)		
10a. Has this individual ever been affiliated with or owned another proprietary school? ☐ No ☐ Yes If yes, please provide full details attached to this application, including any disallowances, fines, or any other disciplinary action against them or the school by any Local, State or Federal authorities.			
10b. Has this individual ever been convicted in this state or elsewhere of a crime, misdemeanor or a felony? ☐ No ☐ Yes If yes, you must submit with this application a written explanation giving the place, court jurisdiction, nature of the offense, sentence and/or other disposition. You must submit a copy of the accusatory instrument (e.g., indictment, criminal information or complaint) and a Certificate of Disposition. If you possess or have received a Certificate of Relief from Disabilities, Certificate of Good Conduct or Executive Pardon, you must submit a copy with this application. Are there any criminal charges (misdemeanors or felonies) pending against this individual in any court in this state or elsewhere? ☐ No ☐ Yes If yes, you must submit a copy of the accusatory instrument (e.g., indictment, criminal information or complaint). Has any license, permit, commission, registration or application for a license, permit, commission, or registration held by you or a company in which you are or were a principal or employee in New York State or elsewhere ever been revoked, suspended or denied by any state, territory or governmental jurisdiction or foreign country, for any reason? ☐ No ☐ Yes If yes, you must submit all relevant documents, including the agency determination, if any.			
If additional partners, attach additional sheets.			
11. Audio/Visual Equipment to be used by school (i.e. PowerPoint, etc.)			
12. Shipping Information In order to provide mandated security guard training, approved security guard training schools and armed guard training schools must utilize Optical Mark Reader (OMR) forms for submission of training information to DCJS. These forms are provided by DCJS; however the school is responsible for the cost associated with shipping the forms. Provide a valid shipping account number with a company of your choosing.			
Shipping Company	Account Number		

New York State Division of Criminal Justice Services
SECURITY GUARD PROGRAM – SECURITY GUARD TRAINING SCHOOL RENEWAL APPLICATION

RA

13. Firearms Training Facility (to be completed by applicant applying for approval to conduct firearms training)		
Name of Range	Type of Range ☐ Indoor ☐ Outdoor	
Street Address	Room/Suite	
City, State, Zip Code	County	
Telephone Number (area code + number)	Facsimile Number (area code + number) (optional)	
Contact Name	Contact Telephone Number (area code + number)	

14. Certified Security Guard Instructors GT= General Topics Instructor / FA= Firearms/Armed Security Guard Instructor (Check all that apply).	Instructor Certifications																								
<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 25%; border-bottom: 1px solid black;">*Social Security Number</td> <td style="border-bottom: 1px solid black;">(Last Name, First Name, MI)</td> <td style="width: 10%; border-bottom: 1px solid black; text-align: center;"> ☐ FA ☐ GT </td> </tr> <tr> <td style="border-bottom: 1px solid black;">*Social Security Number</td> <td style="border-bottom: 1px solid black;">(Last Name, First Name, MI)</td> <td style="border-bottom: 1px solid black; text-align: center;"> ☐ FA ☐ GT </td> </tr> <tr> <td style="border-bottom: 1px solid black;">*Social Security Number</td> <td style="border-bottom: 1px solid black;">(Last Name, First Name, MI)</td> <td style="border-bottom: 1px solid black; text-align: center;"> ☐ FA ☐ GT </td> </tr> <tr> <td style="border-bottom: 1px solid black;">*Social Security Number</td> <td style="border-bottom: 1px solid black;">(Last Name, First Name, MI)</td> <td style="border-bottom: 1px solid black; text-align: center;"> ☐ FA ☐ GT </td> </tr> <tr> <td style="border-bottom: 1px solid black;">*Social Security Number</td> <td style="border-bottom: 1px solid black;">(Last Name, First Name, MI)</td> <td style="border-bottom: 1px solid black; text-align: center;"> ☐ FA ☐ GT </td> </tr> <tr> <td style="border-bottom: 1px solid black;">*Social Security Number</td> <td style="border-bottom: 1px solid black;">(Last Name, First Name, MI)</td> <td style="border-bottom: 1px solid black; text-align: center;"> ☐ FA ☐ GT </td> </tr> <tr> <td style="border-bottom: 1px solid black;">*Social Security Number</td> <td style="border-bottom: 1px solid black;">(Last Name, First Name, MI)</td> <td style="border-bottom: 1px solid black; text-align: center;"> ☐ FA ☐ GT </td> </tr> <tr> <td style="border-bottom: 1px solid black;">*Social Security Number</td> <td style="border-bottom: 1px solid black;">(Last Name, First Name, MI)</td> <td style="border-bottom: 1px solid black; text-align: center;"> ☐ FA ☐ GT </td> </tr> </table>	*Social Security Number	(Last Name, First Name, MI)	☐ FA ☐ GT	*Social Security Number	(Last Name, First Name, MI)	☐ FA ☐ GT	*Social Security Number	(Last Name, First Name, MI)	☐ FA ☐ GT	*Social Security Number	(Last Name, First Name, MI)	☐ FA ☐ GT	*Social Security Number	(Last Name, First Name, MI)	☐ FA ☐ GT	*Social Security Number	(Last Name, First Name, MI)	☐ FA ☐ GT	*Social Security Number	(Last Name, First Name, MI)	☐ FA ☐ GT	*Social Security Number	(Last Name, First Name, MI)	☐ FA ☐ GT	
*Social Security Number	(Last Name, First Name, MI)	☐ FA ☐ GT																							
*Social Security Number	(Last Name, First Name, MI)	☐ FA ☐ GT																							
*Social Security Number	(Last Name, First Name, MI)	☐ FA ☐ GT																							
*Social Security Number	(Last Name, First Name, MI)	☐ FA ☐ GT																							
*Social Security Number	(Last Name, First Name, MI)	☐ FA ☐ GT																							
*Social Security Number	(Last Name, First Name, MI)	☐ FA ☐ GT																							
*Social Security Number	(Last Name, First Name, MI)	☐ FA ☐ GT																							
*Social Security Number	(Last Name, First Name, MI)	☐ FA ☐ GT																							
If additional space is required, attach a separate sheet.																									

15. Intent to Provide Security Guard Training

I intend to conduct the security guard training course(s) checked below in accordance with Part 6027 of the Official Compilation of Codes, Rules and Regulations of the State of New York (9 NYCRR) **using the lesson plans in their entirety provided by the Division of Criminal Justice Services.**

☐ 8 Hour Pre-Assignment Training Course for Security Guards
☐ 16 Hour General On-the-Job Training Course for Security Guards

☐ 47 Hour Firearms Course for Armed Security Guards (Firearms Pistol & Shotgun Course)
☐ 8 Hour Annual In-Service Course for Armed Security Guards (Firearms Pistol Course)

The **school will or has developed its own lesson plans** for the below course(s) in accordance with Part 6027 of the Official Compilation of Codes, Rules and Regulations of the State of New York (9 NYCRR). Attached for each course checked below are the outlines containing topics, objectives and duration for each module of instruction for review and approval by the Division.

☐ 8 Hour Pre-Assignment Training Course for Security Guards
☐ 16 Hour On-the-Job Training Course for Security Guards
☐ 8 Hour Annual In-Service Training Course for Security Guards - **Approved security guard training schools are required to develop lesson plans for the Eight Hour Annual In-Service Course for Security Guards utilizing topics outlined in 9 NYCRR Part 6027.**

New York State Division of Criminal Justice Services
SECURITY GUARD PROGRAM – SECURITY GUARD TRAINING SCHOOL RENEWAL APPLICATION



16. Applicant Affirmation: *This affidavit must be signed and sworn to by the Applicant before a Notary Public.* I hereby affirm, under penalties of perjury, that the information provided in this application is true to the best of my knowledge and belief. I understand that any material misstatement may be deemed sufficient reason to deny approval, or may result in the suspension or revocation of the school approval, if issued. I hereby acknowledge that I have thoroughly read and understand General Business Law section 89-n and Parts 6027, 6028, and 6029 of Title 9 of the NYS Official Compilation of Codes, Rules and Regulations. I further understand that the School Director may have to attend the School Director Orientation Seminar if required by Division of Criminal Justice Services (DCJS) and DCJS may ask for additional information/documentation.

Owner:

Notary Stamp

 Printed Name School Owner

 School Owner's Signature

 Date

Sworn and subscribed before me
 this _____ day of _____ 20____

 Notary Signature

I (school owner) give permission to the Division of Criminal Justice Services (DCJS) to include the school information on the listing of approved security guard training schools made available to the public. ☐ Yes ☐ No

School Director:

Notary Stamp

 Printed Name of School Director

 School Director Signature

 Date

Sworn and subscribed before me
 this _____ day of _____ 20____

 Notary Signature

School Co-Director (if applicable):

Notary Stamp

 Printed Name of School Co-Director

 School Co-Director Signature

 Date

Sworn and subscribed before me
 this _____ day of _____ 20____

 Notary Signature

DCJS Use Only

Application approved: Yes ☐ No ☐ Date: _____

Approved by (printed name): _____ Signature: _____ Date: _____

Comments:



New York State Division of Criminal Justice Services
SECURITY GUARD PROGRAM – TRAINING SITE APPROVAL REQUEST

This form must be submitted to the Division of Criminal Justice Services (DCJS) to receive approval for each school training site. The form provides information on the facilities to determine if they are satisfactory for the proper conduct of mandated security guard training. The facilities must be properly equipped and meet local fire and building standards. At least sixteen square feet must be allotted per student. The Division will identify the number of students allowable for each individual training session based on the square footage of the classroom and equipment etc., located in the space. The number of students allowable in any one training session cannot exceed 35. Training sites used for non firearms security guard training must be handicap accessible. A Certificate of Occupancy; fire authority approval; a floor plan; and digital photographs of the exterior of the premises, building handicap accessibility elements, and interior rooms identified on the floor plan must be submitted with this form. The Division reserves the right to inspect the training site prior to approval.

Certificate of Occupancy

The training site must be approved for use as a school by the municipality in which the site is located. A copy of a valid Certificate of Occupancy must be included with this form. The training site address must be the same as the address listed on the Certificate of Occupancy.

A Certificate of Occupancy (CO) is issued by local municipalities to verify that local building codes have been met and the building is suitable for occupancy. It further states the purpose for which the quarters are to be used (i.e., commercial, residential, school, etc.)

To obtain a copy of a CO in NYC, visit the Department of Buildings' Customer Service Counter in your borough office or log on to the Building Information System at <http://nyc.gov/bis>. If a building was constructed before 1938 and there has been no change in use or additions to the property, it may not have a CO. To obtain proof of the legal use of a building that does not have a CO, you must obtain a "Letter of No Objection" from the Department of Buildings' borough office where the property is located.

*A Certificate of Occupancy is required for all structures; however, certain enterprises may be waived from the requirement that the CO specifically approves the site for school use.

**Submission of a Certificate of Occupancy may be waived for governmental agencies, municipalities and public or private educational institutions in NY or any other jurisdiction.

***If a municipality does not issue Certificates of Occupancy for existing structures, you must submit a letter from the municipality to that effect.

Zoning Compliance Letter

Submit proof that the site to be used to conduct training is legal and is permitted at that location.

*A Zoning Compliance Letter is required for all training sites; however, certain enterprises may be waived from the requirement that the Zoning Compliance Letter specifically approve the site for school use.

**Submission of a Zoning Compliance Letter may be waived for governmental agencies or municipalities and public or private secondary or collegiate-level educational institutions in NY or any other jurisdiction.

Fire Approval

The premises in which mandated security guard training courses will be conducted must be approved for occupancy by the fire authority of the municipality or county in which the site is located. The approval must have been granted during the past three (3) years. The address listed on the fire authority approval must be the same as the address listed in Number 4 (Training Site) of the application. In some circumstances the applicant may not yet have rented the premises. If this is the case, the approval may be missing from the application packet. However, the premises must be rented upon notice to you by DCJS that your approval is nearing completion and Fire Authority Approval must be provided for final approval of the application.

Handicap Accessibility

Training sites used for non firearms security guard training must be handicap accessible. Title III of the American with Disabilities Act (effective January 26, 1992), requires private businesses to be accessible to persons with disabilities. Provide photographs (digital or hard copy) of the handicap accessibility elements of the building.

Floor Plans

Floor plans must be drawn to scale of at least ¼" equaling 1". DCJS reserves the right to request a different scale if necessary. The scale must be indicated on the plans. Each room must be assigned a number and the proposed use of the room and square footage must be listed below (e.g., classroom, bathroom, office, etc.). The floor plans must show:

1. Dimensions of each room or unit of space;
2. Entrances and exits, stairways, corridors, fire escapes;
3. Windows;
4. Student work stations (desks, chairs), furniture, blackboard, white board, audio visual equipment, etc.; and
5. Utilities – heating and air conditioning, and lighting.

*Submission of a floor plan may be waived for governmental agencies or municipalities and public or private secondary or collegiate-level educational institutions in NY or any other jurisdiction.

Photographs

For the training site, digital photographs of the exterior of the premises, building handicap accessibility elements and interior rooms identified on the floor plan must be submitted. Digital photographs must be on a CD/DVD disk or USB flash drive and submitted with the floor plan. For the firearms facility, provide digital photographs of the indoor range (if applicable), the exterior and interior of the classroom(s) and bathroom(s). A floor plan is not required for the firearms facility classroom.



New York State Division of Criminal Justice Services
SECURITY GUARD PROGRAM – TRAINING SITE APPROVAL REQUEST

School Name:	School Identification No:
School Address:	Room/Suite:
City, State, Zip Code:	County:
Telephone Number (area code + number):	
School Owner Name(s):	
School Director Name:	

Training Site Address (if different than above):	
City, State, Zip Code:	County
Training Site Floor Level (e.g., Street level, 2 nd floor, 3 rd floor, etc.):	Is the site handicap accessible: Yes ☐ No ☐

Audio Visual Equipment:

Firearms Facility Name of Range:	
Range Street Address:	County:
City, State, Zip Code:	Range Telephone Number (area code + number):
Range Contact:	Contact Telephone Number (area code + number):
Number of Lanes:	Indoor ☐ Outdoor ☐
Entity that Approved Range:	Facility meets applicable lead safety standards. ☐
Identify safety features of the range (bullet resistant glass, etc.):	

Room Specific Information		
Room Number:	Proposed use of room:	Floor Space in Square Feet:
Room Number:	Proposed use of room:	Floor Space in Square Feet:
Room Number:	Proposed use of room:	Floor Space in Square Feet:
Room Number:	Proposed use of room:	Floor Space in Square Feet:
Room Number:	Proposed use of room:	Floor Space in Square Feet:

_____ Printed Name of Requester (School Owner or School Director only)	_____ Title (School Owner or School Director)
_____ Signature of Requestor	_____ Date

Submit Completed Form to: NYS Division of Criminal Justice Services, Office of Public Safety, Security Guard Program, Alfred E. Smith Office Building, 80 South Swan Street, Albany, NY 12210 Direct questions to the Security Guard Program at (518) 457-4135.

DCJS Use Only	
Floor plan submitted: Yes ☐ No ☐ Date: _____	Digital photographs submitted: Yes ☐ No ☐ Date: _____
Certificate of Occupancy submitted: Yes ☐ No ☐ Date: _____	Zoning Letter Submitted: Yes ☐ No ☐ Date: _____
Fire Approval submitted: Yes ☐ No ☐ Date: _____	
Training site handicap accessible (required for sites to be used for non firearms security guard training): Yes ☐ No ☐ Date: _____	
Number of students allowable per training session based on square footage and equipment etc. located in the space: _____	
Training site approved: Yes ☐ No ☐ Date: _____	
Approved by (printed name): _____ Signature: _____ Date: _____	
Comments:	

New York State Division of Criminal Justice Services
SECURITY GUARD PROGRAM – SECURITY GUARD TRAINING WAIVER APPLICATION

THIS FORM IS USED TO APPLY FOR A WAIVER OF REQUIRED TRAINING FOR SECURITY GUARDS. FORMS PRESENTED FOR FILING MUST CONTAIN ORIGINAL SIGNATURES. ALTHOUGH THE BLANK FORM MAY BE DUPLICATED, PHOTOCOPIES OF COMPLETED FORMS, OR FORMS WITH PHOTOCOPIED SIGNATURES WILL NOT BE ACCEPTED. OMISSIONS OR LACK OF INFORMATION WILL **STOP** THE APPROVAL PROCESS.

The following law enforcement personnel are **exempt** from the 8 Hour Pre-Assignment Training Course for Security Guards, the 16 Hour On-the-Job Training Course for Security Guards and/or the 47 Hour Firearms Training Course for Armed Security Guards and should contact the Department of State, Division of Licensing directly at (518) 474-7569. **DO NOT complete this form.**

- Active Police Officers (as defined by Criminal Procedure Law (CPL) §1.20(34)),
- Former Police Officers*,
- New York State Correction Officers (NYS DOCS) as defined in CPL §2.10 (25).
- Bridge and Tunnel Officers, Sergeants, and Lieutenants from the Triborough Bridge and Tunnel Authority as defined in CPL §2.10 (20),
- Uniformed Court Officers and Court Clerks of the Office of Court Administration as defined in CPL §2.10(21)(a)(b), and
- Sheriffs, Undersheriffs, and Deputy Sheriffs of the New York City Sheriff's Office and sworn officers of the Westchester County Department of Public Safety as defined in CPL §2.10 (2).

Peace officers not specifically named above may apply for a waiver of the 8 Hour Pre-Assignment Training Course for Security Guards, the 16 Hour On-the-Job Training Course for Security Guards and/or the 47 Hour Firearms Training Course for Armed Security Guards.

Peace officers, not specifically named above, seeking a waiver of the 47 Hours Firearms Training Course for Armed Security Guards must be:

1. Authorized to carry a firearm in the performance of their official duties.
2. Been employed in such capacity for at least 18 months.
3. Possess a **valid certificate** awarded pursuant to subdivision six of CPL §2.30 attesting to his or her successful completion of the training requirements imposed by CPL §2.30. A certificate shall remain valid:
 - (a) during the holder's continuous service as a peace officer;
 - (b) for two years after the date of the commencement of a separation of service where the holder had, immediately prior to such separation, served as a peace officer for less than two consecutive years; or
 - (c) for four years after the date of the commencement of a separation of service where the holder had, immediately prior to such separation, served as a peace officer for two consecutive years or longer.

*Police and peace officers who have been retired for more than 10 years at the time of application must complete the 8 Hour Annual In-service Training Course for Security Guards.

Retired or former police and peace officers who are applying for a special armed guard registration card who have not completed initial firearms training within the twelve months prior to employment as a security guard, must complete the 8 Hour Annual In-service Training Course for Armed Security Guards **prior to applying** with the Department of State, Division of Licensing Services.

DCJS reserves the right to require further documentation as necessary to properly classify and/or verify the information and experience contained herein.

SECTION I: APPLICANT INFORMATION

This section must be completed by the applicant. Only individuals who have completed the previous security guard program training or the Basic Course for Peace Officers with Firearms and Deadly Physical Force or Basic Course for Peace Officers and an Initial Firearms and Deadly Physical Force Course may apply for a waiver.

Type or print legibly, the applicant's last name, first name, middle initial, date of birth, Social Security Number, sex, telephone number, address information, and pistol license information. Enter the complete home mailing address, home street address if different, and county of home residence. If the applicant is temporarily living away from home (e.g. enrolled at a college or university, on military assignment, etc.) **DO NOT** list the temporary address. Incomplete submissions will not be processed.

New York State Division of Criminal Justice Services
SECURITY GUARD PROGRAM – SECURITY GUARD TRAINING WAIVER APPLICATION

SECTION II - EMPLOYMENT EXPERIENCE

Fill in the dates and number of years and months worked for any categories being claimed as work experience. **The applicant is required to submit an original letter from the employer verifying employment dates and experience.** Verification of law enforcement employment will be confirmed through the Peace Officer Registry within the Division of Criminal Justice Services.

SECTION III - TRAINING COURSE FOR WHICH APPLICANT IS REQUESTING A WAIVER

Check the box(es) for the courses for which you are applying for a waiver. Documentation requirements are listed below according to employment status. **Submit documentation of pertinent employment only.**

Security Guards

A Security Guard Program course completion certificate verifying satisfactory completion of the 8 Hour Pre-Assignment Training Course for Security Guards and the 16 Hour On-the-Job Training Course for Security Guards and the dates of each course.

Armed Security Guards

Security Guard Program course completion certificates verifying satisfactory completion of the 8 Hour Pre-Assignment Training Course for Security Guards, the 16 Hour On-the-Job Training Course for Security Guards, and the 47 Hour Firearms Training Course for Armed Security Guards and the dates of the course. Please include a photocopy of a valid pistol license issued pursuant to NYS Penal Law §400.00.

Peace Officers

If it has been more than 1 year since the completion of the Initial Firearms Course, former peace officers determined to qualify for a waiver of the 47 Hour Firearms Training Course for Security Guards, **proof of successful completion of the Eight Hour Annual Firearms Course for Armed Security Guards or an MPTC Annual Firearms Course (completed within twelve months of date of application)** must be submitted with the waiver application.

SECTION IV – ATTESTATION

This is an attestation to the accuracy of information supplied on the application. **This must be signed and sworn to by the applicant before a notary public.** Failure to complete this section as required will **STOP** the training waiver process.

MAIL APPLICATION TO:

Where applicable, include the following:

- Original letter from employer verifying employment experience and employment dates (see sample letter).
- Course completion certificate or documentation verifying satisfactory completion with dates of course(s).
- Copy of curriculum with NYS mandated security guard topics, objectives, and number of hours highlighted.
- Persons not authorized by law to carry a firearm as a peace officer must provide a copy of their pistol license when applying for a waiver of the 47 Hour Firearms Training Course for Armed Security Guards.
- Other than this application, **do not submit original documentation** unless specifically requested to do so. Submitted documents will not be returned.

**NYS Division of Criminal Justice Services
Office of Public Safety - Security Guard Program
80 South Swan Street
Albany, NY 12210**

QUESTIONS

If you have any questions regarding this form, call (518) 457-4135 for assistance.

New York State Division of Criminal Justice Services
SECURITY GUARD PROGRAM – SECURITY GUARD TRAINING WAIVER APPLICATION

Sample employment verification letter, to be submitted **on agency/company letterhead**.

Date

NYS Division of Criminal Justice Services
Office of Public Safety - Security Guard Program
80 South Swan Street, Albany, NY 12210

(Applicant Name) has been continuously employed as **(position)** with the **(department/agency name)** from **(start date)** to **(end date)**. They **(are/are not)** authorized to carry a firearm in the performance of their official duties and has been since **(date armed)**.

Our records indicate **(he/she)** has completed annual training in firearms as of **(date of completion)**.

Sincerely,

Agency/Company CEO
Title

New York State Division of Criminal Justice Services
SECURITY GUARD PROGRAM – SECURITY GUARD TRAINING WAIVER APPLICATION



SECTION I - APPLICANT INFORMATION (To be completed by the applicant)

Last Name	First Name	MI	Date of Birth	Social Security Number*	Sex
Home Residence Mailing Address		City, State, Postal Code			
Home Residence Mailing Address (if Different)	City, State, Postal Code		Apt./Suite#	County of Home Residence	
Have you ever been convicted of a crime? ☐ Yes ☐ No		If yes, please explain. Attach another sheet if necessary.			
Home Telephone Number (Area Code First)		Alternate Telephone Number (Area Code First)		Cellular Telephone Number (Area Code First)	

*Pursuant to the New York State Personal Privacy Protection Law, DCJS is authorized to collect personal identifying information as part of a public safety agency record. Personal identifying information on this form shall not be revealed, released, transferred, disseminated or otherwise communicated orally, in writing, or by electronic means other than to the registrant. Disclosure of personal identifying information is voluntary. Refusal to provide personal identifying information shall not result in the denial of any right, benefit, or privilege.

SECTION II – EMPLOYMENT EXPERIENCE

☐ Security Guard Years/mos	☐ Armed Guard Years/mos	☐ Peace Officer (trained and authorized to carry a firearm in the line of duty) Years/mos
An original copy of the letter from the employer verifying dates and type of employment must be included.		

SECTION III – TRAINING COURSE FOR WHICH THE APPLICANT IS REQUESTING A WAIVER

☐ 8 Hour Pre-Assignment Training Course for Security Guards	Course Completed(mm/dd/yyyy)
☐ 16 Hour On-the-Job Training Course for Security Guards	Course Completed(mm/dd/yyyy)
☐ 47 Hour Firearms Training Course for Armed Security Guards	Course Completed (mm/dd/yyyy)
A copy of the course completion certificate for relevant security guard or peace officer training must accompany the application. Persons not authorized by law to carry a firearm as a peace officer must provide a copy of their pistol license when applying for a waiver of the 47 Hour Firearms Training Course for Armed Security Guards.	

SECTION IV – ATTESTATION

Applicant Attestation: This affidavit must be signed and sworn to by the Applicant before a Notary Public. I hereby attest that the information provided in this application is true to the best of my knowledge and belief. I understand that any omission or inaccuracy may be deemed sufficient reason to deny approval. I understand that the Division of Criminal Justice Services may ask for additional information/documentation.

_____ Applicant Signature	Notary Stamp
FOR DCJS USE ONLY Reviewed By: _____	FOR DCJS USE ONLY Date: _____
Sworn and subscribed before me this _____ day of _____ 20____	
_____ Notary Signature	

DCJS USE ONLY	DCJS USE ONLY	DCJS USE ONLY	DCJS USE ONLY
Course Title	Course Dates	School ID#	Year Trained
☐ 700 8 Hour Pre-Assignment	Date (mm/dd/yyyy):		
☐ 701 16 Hour On-the-Job	Date (mm/dd/yyyy):		
☐ 702 47 Hour Firearms Training	Date (mm/dd/yyyy):		
☐ Firearms Training Pending	Date (mm/dd/yyyy):	☐ Current Peace Officer	



SECURITY GUARD TRAINING SCHOOL NOTIFICATION OF CHANGES

Complete Part I for changes to the school information and/or documents. Complete Part II for changes to the School Owner, School Director, School Co-Director or Partner(s). Complete Parts I & II if there are changes to information contained in both parts. Submit Part I and/or Part II to the Division of Criminal Justice Services at the above address. Direct questions to Security Guard Program staff at (518) 457-4135.

PART I

School Name: _____

School Identification Number: _____

CHANGE(S) [Check all that apply and provide information]:

☐ School Name: _____

*For any corporate, limited liability company or limited partnership provide copy of NYS Department of State name availability response.

☐ School Phone Number: _____

☐ School Mailing Address: _____

☐ School E-Mail Address: _____

☐ Type of Ownership - Provide supporting documents for type of ownership.

- ☐ Sole Proprietorship – Provide consent to do business from county clerk
- ☐ Partnership/Limited Partnership – Provide copy of partnership/limited partnership agreement
- ☐ Corporation – Provide Certificate of Incorporation and if applicable, certificate of assumed name
- ☐ Limited Liability Company – Provide copy of Official Filing Receipt
- ☐ Not-for-Profit – Provide Certificate of Incorporation
- ☐ Other – Provide applicable documentation

☐ School Catalog (Attach copy)

☐ Enrollment Agreement (Attach copy)

☐ Payment Receipt Form (Attach copy)

Printed Name of Requester
(School Owner or School Director only)

Title (School Owner or School Director)

Signature of Requestor

Date



New York State Division of Criminal Justice Services
Office of Public Safety/Security Guard Program
80 South Swan Street, Albany, NY 12210

SECURITY GUARD TRAINING SCHOOL NOTIFICATION OF CHANGES

PART II

School Name:	School Identification Number:

☐ **Change to School Owner**

Federal Tax ID Number/Employer ID Number:			
School Owner or Corporation Name:		If Corporation, Contact Name and Title:	
Street Address	City, State, Zip Code	Telephone Number (area code + number)	
If sole owner (proprietor) of school provide the following:			
Gender	Date of Birth	*Social Security Number	Email Address
Has the SCHOOL OWNER ever been affiliated with or owned another proprietary school? ☐ No ☐ Yes			
If yes, please provide full details attached to this application, including any disallowances, fines, or any other disciplinary action against them or the school by any Local, State or Federal authorities.			

Change to (check one): ☐ **School Director** ☐ **School Co-Director** ☐ **Partner**

Name	Gender	*Social Security Number
Telephone Number (area code + number)	Email Address (REQUIRED)	Facsimile Number (area code + number)(optional)
Have you ever been affiliated with or owned another proprietary school? ☐ No ☐ Yes		
If yes, please provide full details attached to this application, including any disallowances, fines, or any other disciplinary action against them or the school by any Local, State or Federal authorities.		

Disclosure (School Owner, School Director, School Co-Director, Partner)

Have you ever been convicted in this state or elsewhere of a crime, misdemeanor or a felony? ☐ No ☐ Yes

If yes, you must submit with this application a written explanation giving the place, court jurisdiction, nature of the offense, sentence and/or other disposition. You must submit a copy of the accusatory instrument (e.g., indictment, criminal information or complaint) and a Certificate of Disposition. If you possess or have received a Certificate of Relief from Disabilities, Certificate of Good Conduct or Executive Pardon, you must submit a copy with this application.

Are there any criminal charges (misdemeanors or felonies) pending against you in any court in this state or elsewhere? ☐ No ☐ Yes

If yes, you must submit a copy of the accusatory instrument (e.g., indictment, criminal information or complaint).

Has any license, permit, commission, registration or application for a license, permit, commission, or registration held by you or a company in which you are or were a principal or employee in New York State or elsewhere ever been revoked, suspended or denied by any state, territory or governmental jurisdiction or foreign country, for any reason? ☐ No ☐ Yes

If yes, you must submit all relevant documents, including the agency determination, if any.

Affirmation: This affidavit must be signed and sworn to by the signer before a Notary Public.

I hereby affirm, under penalties of perjury, that the information provided in this application is true to the best of my knowledge and belief. I understand that any material misstatement may be deemed sufficient reason to deny approval, or may result in the suspension or revocation of the school approval, if issued. I hereby acknowledge that I have thoroughly read and understand General Business Law section 89-n and Parts 6027, 6028, and 6029 of Title 9 of the NYS Official Compilation of Codes, Rules and Regulations. I further understand that DCJS may ask for additional information/documentation.

For School Director: I further understand that as the School Director I must attend the School Director Orientation Seminar if required by the Division of Criminal Justice Services (DCJS).

Notary Stamp

Printed Name

Signature

Date

Sworn and subscribed before me
this _____ day of _____ 20____

Notary Signature

*Attach additional sheets as required



New York State Division of Criminal Justice Services
SECURITY GUARD PROGRAM – TRAINING SITE APPROVAL REQUEST

This form must be submitted to the Division of Criminal Justice Services (DCJS) to receive approval for each school training site. The form provides information on the facilities to determine if they are satisfactory for the proper conduct of mandated security guard training. The facilities must be properly equipped and meet local fire and building standards. At least sixteen square feet must be allotted per student. The Division will identify the number of students allowable for each individual training session based on the square footage of the classroom and equipment etc., located in the space. The number of students allowable in any one training session cannot exceed 35. Training sites used for non firearms security guard training must be handicap accessible. A Certificate of Occupancy; fire authority approval; a floor plan; and digital photographs of the exterior of the premises, building handicap accessibility elements, and interior rooms identified on the floor plan must be submitted with this form. The Division reserves the right to inspect the training site prior to approval.

Certificate of Occupancy

The training site must be approved for use as a school by the municipality in which the site is located. A copy of a valid Certificate of Occupancy must be included with this form. The training site address must be the same as the address listed on the Certificate of Occupancy.

A Certificate of Occupancy (CO) is issued by local municipalities to verify that local building codes have been met and the building is suitable for occupancy. It further states the purpose for which the quarters are to be used (i.e., commercial, residential, school, etc.)

To obtain a copy of a CO in NYC, visit the Department of Buildings' Customer Service Counter in your borough office or log on to the Building Information System at <http://nyc.gov/bis>. If a building was constructed before 1938 and there has been no change in use or additions to the property, it may not have a CO. To obtain proof of the legal use of a building that does not have a CO, you must obtain a "Letter of No Objection" from the Department of Buildings' borough office where the property is located.

*A Certificate of Occupancy is required for all structures; however, certain enterprises may be waived from the requirement that the CO specifically approves the site for school use.

**Submission of a Certificate of Occupancy may be waived for governmental agencies, municipalities and public or private educational institutions in NY or any other jurisdiction.

***If a municipality does not issue Certificates of Occupancy for existing structures, you must submit a letter from the municipality to that effect.

Zoning Compliance Letter

Submit proof that the site to be used to conduct training is legal and is permitted at that location.

*A Zoning Compliance Letter is required for all training sites; however, certain enterprises may be waived from the requirement that the Zoning Compliance Letter specifically approve the site for school use.

**Submission of a Zoning Compliance Letter may be waived for governmental agencies or municipalities and public or private secondary or collegiate-level educational institutions in NY or any other jurisdiction.

Fire Approval

The premises in which mandated security guard training courses will be conducted must be approved for occupancy by the fire authority of the municipality or county in which the site is located. The approval must have been granted during the past three (3) years. The address listed on the fire authority approval must be the same as the address listed in Number 4 (Training Site) of the application. In some circumstances the applicant may not yet have rented the premises. If this is the case, the approval may be missing from the application packet. However, the premises must be rented upon notice to you by DCJS that your approval is nearing completion and Fire Authority Approval must be provided for final approval of the application.

Handicap Accessibility

Training sites used for non firearms security guard training must be handicap accessible. Title III of the American with Disabilities Act (effective January 26, 1992), requires private businesses to be accessible to persons with disabilities. Provide photographs (digital or hard copy) of the handicap accessibility elements of the building.

Floor Plans

Floor plans must be drawn to scale of at least ¼" equaling 1". DCJS reserves the right to request a different scale if necessary. The scale must be indicated on the plans. Each room must be assigned a number and the proposed use of the room and square footage must be listed below (e.g., classroom, bathroom, office, etc.). The floor plans must show:

1. Dimensions of each room or unit of space;
2. Entrances and exits, stairways, corridors, fire escapes;
3. Windows;
4. Student work stations (desks, chairs), furniture, blackboard, white board, audio visual equipment, etc.; and
5. Utilities – heating and air conditioning, and lighting.

*Submission of a floor plan may be waived for governmental agencies or municipalities and public or private secondary or collegiate-level educational institutions in NY or any other jurisdiction.

Photographs

For the training site, digital photographs of the exterior of the premises, building handicap accessibility elements and interior rooms identified on the floor plan must be submitted. Digital photographs must be on a CD/DVD disk or USB flash drive and submitted with the floor plan. For the firearms facility, provide digital photographs of the indoor range (if applicable), the exterior and interior of the classroom(s) and bathroom(s). A floor plan is not required for the firearms facility classroom.



New York State Division of Criminal Justice Services
SECURITY GUARD PROGRAM – TRAINING SITE APPROVAL REQUEST

School Name:	School Identification No:
School Address:	Room/Suite:
City, State, Zip Code:	County:
Telephone Number (area code + number):	
School Owner Name(s):	
School Director Name:	

Training Site Address (if different than above):	
City, State, Zip Code:	County:
Training Site Floor Level (e.g., Street level, 2 nd floor, 3 rd floor, etc.):	Is the site handicap accessible: Yes ☐ No ☐

Audio Visual Equipment:

Firearms Facility Name of Range:	
Range Street Address:	County:
City, State, Zip Code:	Range Telephone Number (area code + number):
Range Contact:	Contact Telephone Number (area code + number):
Number of Lanes:	Indoor ☐ Outdoor ☐
Entity that Approved Range:	Facility meets applicable lead safety standards. ☐
Identify safety features of the range (bullet resistant glass, etc.):	

Room Specific Information		
Room Number:	Proposed use of room:	Floor Space in Square Feet:
Room Number:	Proposed use of room:	Floor Space in Square Feet:
Room Number:	Proposed use of room:	Floor Space in Square Feet:
Room Number:	Proposed use of room:	Floor Space in Square Feet:
Room Number:	Proposed use of room:	Floor Space in Square Feet:

_____ Printed Name of Requester (School Owner or School Director only)	_____ Title (School Owner or School Director)
_____ Signature of Requestor	_____ Date

Submit Completed Form to: NYS Division of Criminal Justice Services, Office of Public Safety, Security Guard Program, 80 South Swan Street, Albany, NY 12210
Direct questions to the Security Guard Program at (518) 457-4135.

DCJS Use Only	
Floor plan submitted: Yes ☐ No ☐ Date: _____	Digital photographs submitted: Yes ☐ No ☐ Date: _____
Certificate of Occupancy submitted: Yes ☐ No ☐ Date: _____	Zoning Letter Submitted: Yes ☐ No ☐ Date: _____
Fire Approval submitted: Yes ☐ No ☐ Date: _____	
Training site handicap accessible (required for sites to be used for non firearms security guard training): Yes ☐ No ☐ Date: _____	
Number of students allowable per training session based on square footage and equipment etc. located in the space: _____	
Training site approved: Yes ☐ No ☐ Date: _____	
Approved by (printed name): _____ Signature: _____ Date: _____	
Comments:	

Appendix R

Deliverable Acceptance Statement for: Public Safety Credentialing and Training System “PSCTS”

Intentionally Blank

DELIVERABLE ACCEPTANCE STATEMENT FOR:
Public Safety Credentialing and Training System “PSCTS”

DATE:

Vendor Name Statement of Submission

Detailed description of items for Acceptance

Vendor Details:

Submitted by:

Name

Title

Signature of Vendor

Date Delivered

Change Order Details, if applicable

Change Order #	Description	Date approved	Comments

NYS Statement of Acceptance

☐ Accepted

☐ Accepted with Exceptions

☐ Not Accepted

Exceptions or Reason for Rejection:

Accepted by:

Name

Title

Signature:

Date:

This Page Intentionally Blank

Appendix S

Training Requirements

Intentionally Blank

Training Requirements

1. The Contractor shall train NYS OPS trainers in all workstation activities, including, but not limited to:
 - a. All user access level functionalities
 - b. Administrator level functions
 - c. All available record transactions
 - d. All available reporting capabilities
2. NYS shall retain final approval authority for all training content.
3. All scheduling for training will be coordinated with and approved by the NYS Office of Public Safety (Director or Designee)
4. The Contractor shall conduct comprehensive classroom training for the NYS administrative personnel before the new system is placed in service.
5. The Contractor shall provide for comprehensive knowledge transfer to NYS ITS technical support staff to enable them to provide ongoing day-to-day support and to help ensure that performance and availability requirements can be maintained.
6. The Contractor shall provide a training plan and training content which includes but is not limited to all requirements defined herein. Should the Contractor training plan include items not defined as required in this document but deemed necessary to fully understand the Contractor solution, that content must be included.
7. The training plan must identify the type of training the Contractor shall utilize to meet each requirement –e.g., Train the Trainer, Computer Based Training (CBT), Hands-on and/or Classroom.
8. The Contractor's instructors shall have extensive knowledge of their proposed solution and be prepared to answer questions on the spot or with a 48 hour turnaround time.
9. The Contractor shall provide training to the NYS trainers within the core working hours of 7:00 AM to 5:00 PM (Eastern Standard Time) on Monday through Friday at the NYS operational facility, in Albany NY.
10. Any and all Training materials developed for purposes herein shall become the exclusive property of the NYS.

11. The Contractor shall provide training support for NYS Trainers as needed.
12. The Contractor shall provide formal training, as needed, upon the occasion of an upgrade or software/hardware update.
13. The Contractor shall deliver the Training materials in electronic format that can be updated by NYS.
14. The Contractor shall train System Administrators and Technical support staff.
15. The Contractor shall provide Training for a minimum of twelve (12) administrators in the following activities, to include but not be limited to:
 - a. Adding, removing users, changing user roles;
 - b. Custom and Ad-hoc reporting
 - c. Managing Administrative Parameters;
 - d. Problem / Error Reporting;
 - e. System Usage Monitoring;
 - f. Systems security;
 - g. System Performance Monitoring Tools;
 - h. Backup and restore operations;
16. The Contractor shall perform daily training assessments to evaluate the effectiveness of its training program. Reports shall be prepared by the Contractor and delivered to NYS no less frequently than daily once the training program has been initiated. Adjustments to the training program shall be made by the Contractor if the evaluation(s) indicated changes are required to improve the effectiveness of training.

Appendix T

Glossary of Acronyms

Intentionally Blank

Abbreviation Definitions

Abbreviation	Definition
BAO	Breath Analysis Operator
CD-ROM	Compact Disc media, read-only memory with a computer data capacity of 650 MB (Megabytes) and compatible with ISO-9660.
CFR	Code of Federal Regulations
CGA	Contracting Government Agency
CGL	Commercial General Liability
CHRI	Criminal History Record Information
CIO	Chief Information Officer
CJIS	Criminal Justice Information Services
COTS	Commercial Off-the-Shelf
CPB	Consumer Protection Board
CPL	Criminal Procedure Law
CPLR	State Civil Practice Law & Rules
CSO	CJIS Systems Officer
DBE	Disadvantaged Business Enterprise
DCJS	Division of Criminal Justice Services
DHSES	Department of Homeland Security and Emergency Services
DOH	Department of Health
DOJ	Department of Justice
DOS	Department of State
DTF	Department of Taxation and Finance (NYS)
EIN	Employer Identification Number
EISO	Enterprise Information Security Office
FBI	Federal Bureau of Investigation
FIRS	Fingerprint Identification Records System
FOIL	Freedom of Information Law
GUI	Graphical User Interface
III	Interstate Identification Index
ISO	Information Security Office, or Insurance Service Office
IT	Information Technology
MBE	Minority Business Enterprises
MPTC	Municipal Police Training Council
NCIC	National Crime Information Center
NYS	New York State
NYSID	New York State Identification Number
NYSP	New York State Police

Abbreviation	Definition
OAG	New York State Attorney General
OITS	Office of Information Technology Services
OLE	Object Linking and Embedding
OMR	Optical Mark Reader
OPS	Office of Public Safety
OSC	Office of the State Comptroller
OSHA	Occupational Health and Safety Administration
PM	Project Manager or Program Manager
PPSI	Personal, Private, Sensitive Information
PSCTS	Public Safety Credentialing and Training System
RFP	Request for Proposal
SA	Security Addendum
SCORM	Sharable Content Object Reference Model
SGP	Security Guard Program
SID	State Identification Number
SOW	Statement of Work
SP	State Police
SS#	Social Security Number
STL	State Technology Law
TPP	Tangible Personal Property
URL	Uniform Resource Locator
USD	United States Dollars
WBE	Women-Owned Business Enterprises
WCB	Worker's Compensation Board (NYS)
WCL	Worker's Compensation Law

Attachment 1

Questions Template

Intentionally Blank

Attachment 1
Questions Template

Vendor Name:	
Address:	
Contact Person Name:	
Telephone #:	
e-Mail Address	

Question Number	RFP Page Number	RFP Part, Section & Paragraph Reference	Question

This Page Intentionally Blank

Attachment 2

DCJS Non-Disclosure Agreement

Intentionally Blank

Attachment 2

Non-Disclosure Agreement

Confidentiality Agreement

This is an Agreement by and between the New York State Division of Criminal Justice Services (DCJS) and/or any other subsequent State agency _____, and the CONTRACTOR (_____.), regarding the consulting services to be performed for DCJS or another State agency by the CONTRACTOR, under Project CJS 2014-01.

CONTRACTOR shall insure that s/he shall abide by all reasonable noninvasive security policies and procedures of DCJS and any other State agency which the CONTRACTOR renders services to in connection with the Project. DCJS and any State agency reserves the right to conduct a security background check on CONTRACTOR, as s/he will have access to confidential information.

New York State law protects the privacy of criminal history, employment, licensing, registry, and certain other State agency records and other confidential information. There may also exist specific State agency site security issues. . CONTRACTOR shall take all reasonable steps required by DCJS and any other State agency to protect confidential information. Additionally, the CONTRACTOR may be required to enter into other non-disclosure confidentiality agreements specific to one or more State agencies to which the CONTRACTOR or his Subcontractors may be rendering services to in connection with this Project.

CONTRACTOR specifically agrees to comply with the "Information Security Breach and Notification Act" as set forth in State Technology Law Section 208 and General Business Law Article 39-F. The CONTRACTOR shall promptly notify the State where there is a reasonable belief of a breach of security, unauthorized access or unauthorized release of personal computer data containing personal information, and take appropriate action with respect to notification of affected individuals and to other required state agencies consistent with the New York State Information Security Breach and Notification Act.

Further, all other information concerning DCJS and any other State agency operations, procedures and policies shall be kept confidential by CONTRACTOR and CONTRACTOR shall comply with any applicable administrative policies, procedures, and other requirements concerning confidentiality.

The use of information obtained by CONTRACTOR in the performance of his duties described herein shall be limited to purposes directly connected with such duties.

The CONTRACTOR shall not remove any work papers or product from DCJS or any other State agency premises except with the written consent of DCJS or such State agency, as applicable, other than work papers brought to the work site by CONTRACTOR which contain no confidential information relating to DCJS, or any other State agency.

CONTRACTOR shall not be required to keep confidential any such material which is publicly available through no fault of CONTRACTOR, independently developed by CONTRACTOR without reliance on confidential information of DCJS, or otherwise obtained under the Freedom of Information Law or New York State laws or regulations.

The prohibition against disclosure shall survive the termination of this Agreement, the termination of the SOW or the completion of the SOW.

This Agreement is made and will be construed in accordance with the State of New York.

IN WITNESS WHEREOF, the Parties hereto have caused this Agreement to be executed as of the date indicated below.

	<u>NYS Division of Criminal Justice Services or other State agency.</u>
Signature:	Signature:
Name (Please Print)	Name (Please Print)
Title:	Title:
Date:	Date:

ACKNOWLEDGMENT CLAUSE

State of _____)

) ss.:

County of _____)

On the _____ day of _____ in the year 20_____ before me personally came _____ to me known, who, being by me duly sworn, depose and say that s/he is the _____ of the entity which executed the above instrument; that s/he was authorized by and did execute the same at the direction of said entity and that s/he signed his/her name thereto.

Notary Public: _____

Attachment 3

Not Used Intentionally Blank

Intentionally Blank

Attachment 4

Not Used Intentionally Blank

Intentionally Blank

Attachment 5

Offerer Firm Information Form

Intentionally Blank

Attachment 5

Offerer Firm Information Form

Public Safety Credentialing and Training System Request for Proposals CJS 2014 01
Name of Company Bidding:
Offerer Firm's Federal Tax ID Number:
Street Address:
State:
City:
Zip:
County:
Country:
Contact Name:
Title:
Phone Number:
Fax Number:
Toll Free Phone Number:
Toll Free Fax Number:
Email Address:
Corporate Website:

Attachment 6

Mandatory Qualifying Experience

Customer Reference Form

Intentionally Blank

Attachment 6

Mandatory Qualifying Experience Customer Reference Form

Public Safety Credentialing and Training System Customer Reference

Offerer/Firm Name: _____

Proposed Software Release/Version: _____

Qualifying Reference(s) Instructions:

The Offerer must provide all contact information and qualifying data for a minimum of two (2) customers, organizations not controlled or owned by the Offerer, in the past five years for which the Offerer, as Contractor, has successfully implemented a PSCTS or similar system that has been in production for at least 90 days, currently utilizing software release/version that is within one major release from the proposed and where all hosting services are provided by the Customer, as described below. If all components or features listed below have not been installed at a single location, Offerer may provide additional customer references up to a maximum of seven (7) to document their experience in providing all required components or features listed in section 3.1.B, provided that a) the first four criteria (1. Annual Validation; 2. Gap Analysis and Validity, 3. Self Service Functionality and 4. Reporting), have been installed at one or more single location(s), and b) that all criteria have been met through a combination of one or more of the customer references.

NYS may contact, by mail or by phone, all of the customer references provided by the Offerer to request a response to the Customer Reference Questionnaire contained in Appendix F.

Please provide the information requested in the attached Mandatory Qualifying Experience and Customer Reference chart. Mandatory qualifying experience items 1-8 are as follows:

1. Allows employers to perform annual validation of all employment records and report the results to records management staff; employers are able to input, update, and validate details specific to each individual employed by them currently and in the past (“Annual Validation”).
2. Provides Gap Analysis of the validity and pending expirations of training certificates and/or qualifications; identifies gaps in employment service (including from one employer to another); and provides notification of pending expirations of certificates and/or qualifications to employers, individual record holder(s) and records management staff (“Gap Analysis and Validity”).
3. Provides self-service functionality for employees (view access for records and certificates), employers (records and data management), training instructors and academies (training record management), and administration (configuration), application is user friendly to the average non-technical individual (“Self Service Functionality”).

4. System generates standard reports and statistics, including gap analysis; performs audits of training certificates and actions of system users; and the ability to define and generate ad hoc reports exists. Reports can be generated in standard formats including Adobe PDF and Microsoft Excel (“Reporting”).
5. Has a database of at least 50,000 personnel records and is capable of supporting 150 concurrent users; vendor support is available at a minimum Monday to Friday during business hours.
6. Performs a minimum of 100,000 transactions (records updates) annually and the application’s user interface provides feedback in 5 seconds or less, from each key press, mouse movement or other type of input or exchange.
7. System has interfaces with at least one (1) exterior agency/entity e.g. FBI, State Police, Department of Health, wherein data imports and exports occur; the interface is user friendly to the average non-technical individual and capable of self service features including bulk-upload capabilities
8. Contains an on-line portal or equivalent component that automates processes for course enrollment, approval and completion, records management, certificate issuance; includes features including ability to approve and manage training academies, document retention and management, training course calendaring and self-service functionality for instructors and students. The system must allow NYS to upload training materials (records management) including but not limited to text files, audio files and/or video files with individual files upwards of 4GB in size. System must be capable to develop, manage, provide and administer distance learning course offerings allowing for up to 1,500 concurrent users. System must support SCORM and ASCII compliant software.

Attachment 6
Mandatory Qualifying Experience and Customer Reference Chart
Offerer Response Form

Customer Reference and System Information	Reference 1	Reference 2	Reference 3	Reference 4	Reference 5	Reference 6	Reference 7
Reference Name and Contact Information (please provide contact name, title, phone number, e-mail and contact hours with time zone)							
Offerer primary contractor? (must be yes)							
Date system placed in production (must be at least 90 days, maximum 5 years)							
Software Release/Version currently in use							
Customer Hosted (not vendor hosted) Y/N?							
Customer Reference controlled or owned by offerer Y/N? (must be No)							
Meets mandatory qualifying experience?	Reference 1	Reference 2	Reference 3	Reference 4	Reference 5	Reference 6	Reference 7
1							
2							
3							
4							
5							
6							
7							
8							

Attachment 7

Public Safety Credentialing and Training System “PSCTS”

Mandatory Base System Requirements – COTS or Customized

Intentionally Blank

Vendor:			
For each of the <u>MANDATORY</u> requirements specified below, enter check mark in the appropriate box to specify whether the proposed PSCTS solution meets the <u>MANDATORY</u> requirement as part of the proposed COTS PSCTS solution or as a customization to the proposed COTS PSCTS solution. If customization of the COTS PSCTS system must be done for any part of a requirement, mark the "Customized" box. If all components of the requirement are in the COTS system, mark the corresponding COTS box.			
Requirement # referenced in RFP Section 3.1.C	System Requirement	COTS	Custom
2	The proposed system must Maintain and secure Personal, Private, Sensitive Information ("PPSI") inclusive of dates of birth (DOB) and Social Security Numbers (SS#). The Offerer's PSCTS must be capable of utilizing a secure internet connection to safely transmit personal protected information to NYS.		
3	The Offerer shall supply all software required to implement its solution including interfaces, the test environment, and technology refresh including the Production and Test environment COTS Products.		
4	The Offerer shall propose a PSCTS initially capable of processing a minimum of 100,000 personnel transactions (record updates) annually. The system shall be capable of expanding transaction capacity and records storage capacity by ten percent each subsequent year.		
5	The Offerer shall propose a PSCTS capable of maintaining a training history for 1,000,000 individual training records.		
6	The proposed system must be initially capable of supporting 150 concurrent users.		
6	The proposed system must be capable of vertical and horizontal scaling to allow for system expansion.		
7	Vendor support for the system will be, at a minimum 5x12 (Monday to Friday 6:00 AM to 6:00 PM)		
8	The Offerer shall provide a PSCTS test environment at the NYS that: A. has all features and functionality of the proposed production system B. is independent of and mirrors the production system C. is smaller in size and capacity than the production system, but shall have all software components, providing for a test system sized to at least 5% of the production databases(s), files, and queues with comparable throughput and capacity D. can be utilized by NYS staff to verify and quality assure all new vendor releases and system patches before		

	deployment to the NYS production system E. can be utilized by NYS development team to test changes in NYS software that communicates with the PSCTS.		
9	Vendor will have a representative on-site for all phases of system installation.		
10	The PSCTS user interface must provide feedback in less than 5 seconds after each key press, movement of the mouse, or any other physical input from the user, and after each change in the state of controls that react to input from the user, for example, displaying menus or indicating drop targets.		
11	Proposed system will allow the combined records management of two separate customer populations; the Police and Peace Officer Registry and the Security Guard Program. Both populations must be capable of performing maintenance of records applicable to their assigned responsibilities. See Appendix K Table 2, Population for a list of the designated users.		
12	The Offerer shall encrypt all NYS data, residing or in communication outside the NYS internal network and OFT datacenter, with a minimum 128 AES encryption. In addition, the system must have CJIS and FIPS 140-2 certification. This includes backup media, file transfers and external sites. NYS shall be given all cryptographic keys used involving NYS data and systems.		
13	Proposed system will be a multi-functional solution that combines a Records Management Database and a Training Management system		
13 & 39	Proposed system will be a multi-functional method to create standard and ad hoc reports & statistics, perform audits of training certificates, and audits of the actions of system users.		
14	Conversion Plan Requirements – See Appendix L		
15	The proposed solution shall support the following internet browsers: A. Microsoft Internet Explorer, versions 9 and 10 and any version released after 01-January-2014. B. Apple Safari, versions 4, 5, 6 and 7 and any version released after 01-January-2014. C. Firefox, versions 10 through 25 and any version released after 01-January-2014. D. Google Chrome, versions 2 through 31 and any version released after 01-January-2014.		
16	The Offerer's PSCTS design shall include, at a minimum:		

	A. Hardware specification that is consistent with ITS portfolio of supported platforms listed in Appendix P. B. Software for all workflow, processing, and interface messaging to DCJS, DOS, DOH, NYSP, DHSES and NYS external partners (customers); C. Files and database requirements; D. Data storage requirements; E. Software; F. Algorithms for searching and processing G. Interoperability for internal and external partners, now and in the future.		
17	The proposed solution will, to the maximum extent possible, automate all business processes listed in Appendix K Table 3.		
18	The proposed solution must keep to a minimum processes which require the exchange of paper or dependency on the vendor (e.g. reports).		
19	User interface and data input must be user friendly to the average, non-technical individual and capable of self service at the Employer level. Requirements include: A. Bulk upload features with real-time feedback to user for data correction. B. User specific drop down fields C. Automated calendaring D. All opportunities to limit or eliminate manual typing (thus limiting opportunities for typographical errors)		
20	System must provide the ability to allow the provider of training to review records of classes they or their agency/firm provided.		
21	System must allow local agency training coordinators to access all training records of agency staff regardless of the provider of that training.		
22	System must reduce the number of clicks required to submit or enter data. Pages containing information required for specified processes must have all details on one page. One example is the Annual Police Officer Registry update process which should have all required information contained in one page or screen, thus reducing time spent and opportunities for error created by navigating to various places in the application. A second example is completing training course information such as curriculum content forms and class rosters.		
23	The proposed solution shall allow NYS to control user access and customize user's ability to edit records. For example, each individual system user must be allowed to update his or her personal contact information such as a phone number and or		

	email address and have privileges to view and print training certificates and records. While other users such as a Chief of Police can access all training with the ability to edit all records of training provided by his or her organization. The total current user population is listed in Appendix K, Table 2, Population and expected levels of access of each user level are listed in Appendix K Table 4 User Access Levels.		
24	Interface with State systems to provide for the exchange of data for examples with NYS Department of State (DOS), Department of Health (DOH), State Police (SP) and Division of Homeland Security and Emergency Services (DHSES). Ideally, these interfaces should provide the ability to interact as a web service between NYS and partner agencies. See Appendix K Table 4, User Access levels for more information.		
Records Management Requirements:		COTS	Custom
25	Proposed system will assign each personnel record and each user agency or employer a unique identifier to be used as a customer account number when accessing the system.		
26	Proposed solution will maintain a history for all training courses recognized by NYS. Currently, NYS recognizes 430 training courses and maintains data for every occurrence of the 430 courses. The proposed solution must allow NYS to continue to capture historical course data that includes; location, attendees, instructor(s), curricula, length of instruction in hours, and the NYS staff actions taken to review and approve each course. NYS's current Ingenium interface labels training courses as "Learning Experiences." The 430 Learning Experiences (Training Courses) are listed in Appendix K, Table 5.		
27	The proposed solution must be capable of expansion to accommodate the addition of new Learning Experiences and new categories of police and peace officers. Refer to Appendix K, Table 5 for a listing of the current Learning Experiences and Appendix K, Table 9, CPL Definitions for Peace Officers and Appendix K, Table 10, CPL Definitions for Police Officers		
28	Proposed system allows for recording employment history of officers who have multiple job titles and the capacity in which they serve each employer. Additionally, the proposed system should be capable of maintaining a rank history throughout the officer's career.		
29	The proposed solution will contain a Police and Peace Officer Registry database that is integrated and linked to the training provided by employers, academies and NYS. -		

30	Proposed solution will contain a Security Guard Training Records Database that is integrated and linked to the training provided by employers, academies and NYS. -		
31	Proposed System will allow employers of persons on the Police and Peace Officer Registry to self-service employee's records. Employers must be able to input, update, and validate details specific to each individual employed by them currently and in the past. In addition to the as needed records maintenance of assigned personnel, employers are required perform an Annual Validation of all their employees in the Police and Peace Officers Registry database. The specific details of the current processes for as needed or real-time registry changes are described on Appendix I.9, <i>Police and Peace Officer Registry Processes</i> . The current process for Annual Validation is described in Appendix I.10, <i>Annual Validation Process</i> .		
32	Proposed solution will allow NYS to administer a course approval and completion process for training courses administered by local training academies. This core business function is known as Course Approval. The specific details of the desired Course Approval and Completion Processes are depicted in flowcharts located in Appendix I.2 & I.3. The current processes for Course Approval, Course Completion, and Data Recording are depicted in Appendices I.4, I.5, and I.6, respectively. The system must Allow NYS to capture all data fields and/or data points currently captured in all hardcopy and or web based forms. These forms may be found in forms appendix.		
32	The proposed solution must include a process for NYS to process applications by new Security Guard Schools. NYS must be able to receive, review and approve new applications as well as renewal applications.		
Records Management Requirements (Continued):		COTS	Custom
33	NYS currently receives completed Security Guard Training Data on Optical Mark Reader (OMR) bubble sheets that are scanned in. Proposed Solution will allow for the importing of Security Guard training data from a flat-file format. The current method for recording completion of security guard courses utilizes Optical Mark Reader (OMR) forms completed by the students and mailed to NYS by the school director. NYS staff utilizes a Pearson Op-Scan to collect the student data from the schools. The current system uses Object Linking and Embedding (OLE) technology to capture the data. The data is then converted to a flat-file format for import into the Ingenium database and for daily export to NY Department of State (DOS). DOS requires the information must receive the course has time requirements to process the NYS processes thousands of these OMR forms every month and DOS is mandated to process time constraints on it is anticipated		

	1. Currently Security Guard employers submit course completion documentation in the form of Optical Mark Reader (OMR) bubble sheets which are scanned in on a Pearson Op-Scan. The data is then transferred to a flat-file which is imported into the Ingenium database and also transmitted to the Department of State each day. in The proposed solution will allow for the processing of data from Optical Mark Reader (OMR) bubble sheets submitted by Security Guard Program Employers. Employers submit course completion documentation from Security Guard Schools in the form of OMR (bubble sheets) that are scanned in. The current Security Guard Training process and details of the data submitted by OMR bubble sheets is depicted in a flowchart located in Appendix I.15. NYS envisions that the self service functionalities provided by the proposed solution will obviate the need for the aforementioned OMR process however the proposed solution must enable NYS to continue the OMR process for an indeterminate period post implementation to allow for an acceptable cut-over period for external customers.		
34	Proposed solution will provide a self-service model allowing Security Guard Instructors to submit initial applications as well as recertification applications every five years.		
35	Proposed solution will enable the training history of an officer, from recruit to retirement, to be recorded and accessible. The training history of each individual must follow all individuals regardless of change in Employer(s), or name(s). These histories must be accessible to authorized persons requiring access to this information such as record holder(s), employers, and NYS. The ability to meet the Agency Requirement is non-negotiable, the solution of how this requirement is met, is negotiable.		
Training Management Requirements:		COTS	Custom
36	Proposed solution will allow for the administration of training course material for traditional in-residence classroom instruction provided by NYS staff, contract instructors, academies, and employers.		
37	Proposed solution shall include a training course calendar that: a. allows NYS to assign or customize pre-requisites for course enrollments. b. limits users ability to enroll in courses based on pre-requisites c. allows self-registration by users. d. generates customized registration approval or disapproval notices based on pre-requisites. e. issues certificates upon course completion, and		

	f. performs records management updates upon course completion. Refer to Appendix K, Table 5, Learning Experiences, for a listing of current training courses and corresponding course pre-requisites.		
Reports, Statistics & Audits Requirements:		COTS	Custom
38	The proposed solution shall include a means to produce configurable reports, as described in Appendix K, Table 1, Report Requirements. Also, this solution will allow for NYS' ad hoc reporting.		
39	NYS requires a solution that will identify gaps in the validity and expiration of training certificates and identify gaps in an officer's service from one employer to another.		
40	The system must be able to record, maintain and report on each officer's rank history, including transitions from one employer to another or from multiple employers and roles.		
41	Proposed system will have a method to suppress and secure records of undercover officers and other individuals with similar requirements. Minimal, if any, workarounds are anticipated, processes must not be onerous.		
39	Proposed solution shall record and log history of changes made by internal and external users.		
42	Proposed solution shall deliver Reports in standard formats to include Adobe PDF and Microsoft Excel.		
43	Proposed solution shall provide a reminder function to NYS Administrators and employers for due or overdue reports.		
44	Proposed solution shall provide access by other state entities to verify and/or extract data. These users are identified in Appendix K Table 2 Population and their expected access is identified in Appendix K Table 4 User Level Access.		
45	Proposed solution provides capability to produce standard and ad-hoc reports on specific courses to include; geographic location held course providers/instructors Date and time course was held number of courses held in a specific region		
46	Proposed solution has ability to provide reports on student evaluations of training courses.		
47	Proposed solution is capable of storing sample lesson plans, model training policies/memorandums and forms in Microsoft Word and PDF formats that can be downloaded by customers.		
48	Proposed solution must include documentation describing system functionality including Use Cases and requirements		

57	The Prime Contractor shall produce Production Reports which include, but are not limited to, the Reporting Requirements specified in Appendix K within a mutually agreed upon timeframe after contract approval for NYS approval.		

Attachment 7a

Public Safety Credentialing and Training System “PSCTS”

Optional Features – COTS or Customized

Intentionally Blank

Attachment 7a

PSCTS Optional Features – COTS or Customized

Vendor: For each of the optional features specified below, enter check mark in the appropriate box to specify whether the proposed PSCTS solution a) provides the option as part of the proposed COTS PSCTS solution (“COTS”) or b) can provide the option as a customization to the COTS PSCTS solution (“Customized”) or c) does not provide the option (“N/A”).				
Item Number	Optional Feature	COTS	Custom	N/A
1	System shall provide all capabilities required for NYS to establish an online or portal based learning management system. System shall allow NYS to develop, manage, provide and administer distance learning course offerings allowing for up to 1,500 concurrent users. System must support SCORM and ASCII compliant software. System must allow for use of individual training files in excess of 5GB.			

This Page Intentionally Blank

Attachment 8

**PSCTS Mandatory Base System
Requirements – Solution and/or
Documentation Descriptions with Forms
Required for Offerer Bid Response**

Intentionally Blank

Attachment 8

PSCTS Mandatory Base System Requirements - Solution and/or Documentation Descriptions with Forms Required for Vendor Bid Response

Vendor:	

For each solution or document item in this attachment, the vendor respectively must provide a response. The descriptive response for each shall address, at a minimum, the points specified. Use as much space as necessary to define and clarify your responses, attaching additional pages to these Vendor Bid Response forms in your response with Item Number clearly identified.

Scoring Legend:

- 0 = Vendor's response did not adequately address the issue in question to any degree, and/or would be considered completely unsatisfactory.
- 1 = Vendor's response addressed the issue in question to only a very limited degree, and/or would be considered minimally satisfactory.
- 2 = Vendor's response addressed the issue to an adequate degree and/or would be considered an average response.
- 3 = Vendor's response addressed the issue to a better-than-adequate degree, and/or would be considered a good response.
- 4 = Vendor's response addressed the issue to a significant degree, and/or would be considered a very good response.
- 5 = Vendor's response addressed the issue to a superior degree and/or would be considered an excellent response

Attachment 8

**PSCTS Mandatory Base System Requirements - Solution and/or Documentation Descriptions with Forms
Required for Vendor Bid Response**

A. System Solution/Documentation	
Item A.1.	The proposed solution must conform to NYS Office of Information Technology Services (ITS) requirements. Describe the proposed solutions compatibility with each of the below listed ITS supported environments. a. Proposed Operating System shall be one of the following: 1) IBM POWER AIX 2) Red Hat Enterprise Linux 3) Microsoft Windows Server b. Proposed Database (RDBMS) shall be one of the following: 1) Oracle 2) MS SQL 3) DB2 c. Proposed Web Servers shall be one of the following: 1) Apache 2) Microsoft IIS 3) IBM HTTP 4) RedHat HTTP d. Proposed Application Servers shall be one of the following: 1) J2EE i) WebSphere Application Server ii) JBOSS iii) Oracle WebLogic 2) .NET - - Microsoft IIS e. Proposed Solution shall operate with the NYS ITS Authentication and Authorization Services This service is based on LDAP and supports SAML and Netegrity SiteMinder to access the NYS Statewide Directory. f. If Mainframe Services are proposed, the solution must be supported by either z/OS or z/Linux Proposed solution shall be able to run effectively within a virtual server environment running on an approved operating system (see above).
The Offerer's solution description must be provided below and on additional pages, if necessary:	
Solution Description:	
Evaluation Comments:	

Attachment 8

PSCTS Mandatory Base System Requirements - Solution and/or Documentation Descriptions with Forms Required for Vendor Bid Response

A. System Solution/Documentation	
Item A.2	Describe how the proposed system will convert legacy data for organizations, individuals, training records, certifications, etc. currently on several systems into one database and create one searchable record for each individual. System Information is listed in Appendix G, <i>Peace and Police Registries Informational Tables</i> and Appendix K, <i>OPS Business Needs</i> .
The Offerer's solution description must be provided below and on additional pages, if necessary:	
Solution Description:	
Evaluation Comments:	

A. System Solution/Documentation	
Item A.3	NYS will require the selected offerer to provide detailed plans for reliability acceptance testing and all plans must be approved by NYS prior to acceptance testing. The Offerer's plan(s) shall specifically address the elements of a) the application, b) quality assurance processes, c) performance, and d) accuracy. 1. Describe key features of the proposed solution's reliability acceptance testing plan(s) and specifically address each of the elements below; a. application, b. quality assurance processes, c. performance, and d. accuracy. 2. Also address how the plan will determine the expected results and validation techniques for: a. accuracy b. throughput c. functionality, and d. interoperability
The Offerer's solution description must be provided below and on additional pages, if necessary:	
Solution Description:	
Evaluation Comments:	

Attachment 8

PSCTS Mandatory Base System Requirements - Solution and/or Documentation Descriptions with Forms Required for Vendor Bid Response

A. System Solution/Documentation	
Item A.4	NYS requires a system that will allow its staff to make documents available to customers such as approved lesson plans, PowerPoint, forms, applications, model policies and regulations. Describe how the proposed system will accommodate document storage and retrieval and specifically address; a. capability to accommodate MS Word/Excel/PowerPoint and Adobe@ PDF documents. b. capability to accommodate documents up to 4 GB in size. c. capability of NYS Staff to upload/store documents in the system. d. capability of customers to download documents. Describe limitations, if any on the size, quantity or scale of individual files or documents capable of being stored by your system
The Offerer's solution description must be provided below and on additional pages, if necessary:	
Solution Description:	
Evaluation Comments:	

Attachment 8

PSCTS Mandatory Base System Requirements - Solution and/or Documentation Descriptions with Forms Required for Vendor Bid Response

A. System Solution/Documentation	
Item A.6	NYS requires a solution that allows secure and customizable access to eleven (11) levels of users. DCJS also requires a solution that is capable of supporting users that may perform multiple roles for an employer and/or work for multiple employers. A description of the required levels of users is in Appendix K.4, <i>User Access Levels</i>. Note: Offerer responses to items a-f below do not require a specific answer to each of the 11 User Access Levels listed in Appendix K.4. The written response must address the proposed systems capability, limitations and solutions to meet all the User Access Levels desired as well as the desired capability to support users that perform multiple roles for an employer and user that may work for multiple employers. If the proposed solution is incapable of providing any item(s) in Appendix K.4 as well as any item(s) listed below in a-f, then those item(s) must be specifically addressed in the response. Describe the proposed systems; a. capability to provide access to all users listed in Appendix K.4 b. limitations, if any, in providing access to all users listed in Appendix K.4 c. capability to support users that may have multiple roles for their employer . For example, a police officer may be employed full-time by a police department and require level 1 access, as described in Appendix K.4. This person may also serve as the training officer (level 2 access) for that department. This officer would need access commensurate with the job that could include the ability to update records of employees assigned to the department. d. capability to support users that work for multiple employers. For example, an user may be employed a police officer and require level 1 access and be employed part -time as a security guard with another employer and would require level 6 access. Describe anticipated problems or concerns, if any, with records management. e. capability to manage records access for individuals with no affiliation to law enforcement. One example is the civilian security guard trainees that are not sworn officers or peace officers. Training is a pre-cursor to employment as a security guard and access to individual records by persons that have not been trained and/or certified is a concern. f. security solutions to support secure access to all users described in Appendix K.4
The Offerer's solution description must be provided below and on additional pages, if necessary:	
Solution Description:	
Evaluation Comments:	

Attachment 8

**PSCTS Mandatory Base System Requirements - Solution and/or Documentation Descriptions with Forms
Required for Vendor Bid Response**

<i>B. Records Management Solution/Documentation</i>	
<i>Item B.1.</i>	Describe how the proposed system will use unique identifiers or customer account numbers to enhance security, as required in Section #3.2.C
The Offerer's solution description must be provided below and on additional pages, if necessary:	
Solution Description:	
Evaluation Comments:	

Attachment 8

**PSCTS Mandatory Base System Requirements - Solution and/or Documentation Descriptions with Forms
Required for Vendor Bid Response**

B. Records Management Solution/Documentation	
Item B.2	NYS's current system allows staff to search the database and retrieve records by the following categories; describe how your system can retrieve data by, but not limited to, the following categories: 1) People: Searches all individual officer/employee records (See Appendix K.2, User Population) 2) Agencies: All employers of persons in the database (See Appendix K.2, User Population) 3) Learning Experiences: The 430 individual training courses that are approved by NYS (See Appendix K.5, Learning Experiences), and 4) Events: The actual training courses (Learning Experiences) conducted by employers and reported to NYS. Any proposed solution will need to accommodate NYS's current search categories for records or offer a comparable/equivalent system for records management. Describe how the proposed solution: a. will allow the integrated management of records for People, Agencies, Learning Experiences and Events. b. will update the records for People completing a Learning Experience and the associated Agency records, as needed. c. is integrated and expandable to meet future needs such as the creation of new categories of police or peace officers, the addition of new Learning Experiences, new Agencies, and associated Events.
The Offerer's solution description must be provided below and on additional pages, if necessary:	
Solution Description:	
Evaluation Comments:	

Attachment 8

PSCTS Mandatory Base System Requirements - Solution and/or Documentation Descriptions with Forms Required for Vendor Bid Response

B. Records Management Solution/Documentation	
Item B.3.	Describe how the proposed solution will allow NYS Staff to customize prerequisites to training courses. Include in the response how the proposed solution will automate the process and will enable students, employers and NYS Staff to determine whether a student is authorized, eligible, or ineligible to enroll in a certain training course. Also include in the response whether the proposed solution can automate and or accommodate for the following prerequisite scenario. The NYS Crash Management Courses are a progressive series of four training courses. Students are required to achieve a 70% score to pass the Basic Crash Management Course (Course Code 039); however an 80% minimum score is a prerequisite for a student to advance and enroll in the next level of training; Intermediate Crash Management (Course Code 040). Students are required to achieve a 70% score to pass Intermediate Crash Management and again require an 80% minimum score to enroll in the next level of training – Advanced Crash Management (Course Code 041).
The Offerer's solution description must be provided below and on additional pages, if necessary:	
Solution Description:	
Evaluation Comments:	

B. Records Management Solution/Documentation	
Item B.4	NYS maintains records for two different customer populations, a) Police and Peace Officer Registry records and b) Security Guard Training records database. Access to the training records is different based on the needs of the sworn Police Officers and the civilian Security Guards. Describe how the proposed solution would allow for the records management of the two distinct populations (Peace and Police officers and Security Guards). Include any challenges and/or security risks the multi-use registries may pose.
The Offerer's solution description must be provided below and on additional pages, if necessary:	
Solution Description:	
Evaluation Comments:	

Attachment 8

PSCTS Mandatory Base System Requirements - Solution and/or Documentation Descriptions with Forms Required for Vendor Bid Response

B. Records Management Solution/Documentation	
Item B.5	The proposed solution must enable employers of persons on the Police and Peace Officer Registry to self-service employee's records pursuant to mandatory requirements as specified in Section 3.2.C. items 28, 32, 33 & 41. A. Describe how the proposed system will automate the real-time Police and Peace Officer Registry processes described on Appendix I.9. Specifically address how the proposed solution will; 1. eliminate all paper based and manual data entry functions described in Appendix I.9. 2. allow employers to input, update, and validate details specific to each individual currently employed 3. allow employers to make changes to records of past employees 4. allow NYS staff to approve changes that add or remove employees from the registry. B. Describe how the proposed system will automate the Annual Validation process described on Appendix I.10. Specifically address how the proposed solution will; 1. eliminate all paper based and manual data entry functions described in Attachment I.10. 2. allow employers to perform and submit an Annual Validation of all their employees in the Police and Peace Officers Registry database. 3. allow NYS staff to approve changes that add or remove employees from the registry. 4. will track employer compliance and progress with the Annual Validation requirement 5. will report the results to NYS by January 15th each year.
The Offerer's solution description must be provided below and on additional pages, if necessary:	
Solution Description:	
Evaluation Comments:	

Attachment 8

**PSCTS Mandatory Base System Requirements - Solution and/or Documentation Descriptions with Forms
Required for Vendor Bid Response**

B. Records Management Solution/Documentation	
Item B.6.	NYS manages records relevant to law enforcement training courses administered by local training academies. These core business functions are known as Course Approval and Course Completion. NYS desires a Course Approval and Course Completion process as depicted on flowcharts in Appendix I.2 and I.3. NYS's current processes for Course Approval, Course Completion, and Data Processes are depicted on flowcharts located in Appendix I.4 - I.6. NYS requires a solution that will automate the current processes for Course Approval and Course Completion. Describe how the proposed system will automate and allow; A. external providers to submit proposed courses and instructors for NYS pre-approval. B. NYS to review and approve the proposed training course and generate approval or disapproval notifications to the external provider. C. external providers to submit rosters and course completion documents for approved courses to NYS for processing. Of importance is how the system allows data entry and interfaces with external systems rosters. D. NYS to audit the course rosters and documents for completeness and update individual records for trainees, instructors, employing agency and external providers. E. generation and distribution of course completion certificates, as required.
The Offerer's solution description must be provided below and on additional pages, if necessary:	
Solution Description:	
Evaluation Comments:	

Attachment 8

PSCTS Mandatory Base System Requirements - Solution and/or Documentation Descriptions with Forms Required for Vendor Bid Response

B. Records Management Solution/Documentation	
Item B.7.	NYS approves applications for new Security Guard Schools as well as renewal applications every two years. The current application process requires a fee to be submitted to the NYS finance office along with the application and supporting documents. Once the payment is approved by Finance, the application and supporting documents are forwarded to OPS staff for verification and processing. NYS is not expecting a proposed solution to handle the financial aspect of the process, however, an automated solution to the process for school application and renewal is mandatory. Describe how the proposed solution will encompass: a. initial school applications b. two year recertification of schools c. automated reminders for pending or expired school certifications d. employers to enter new employee records into the records system in a self-service model e. distinguish between For-profit and Not-for-Profit Security Guard Schools to avoid charging fees to Not- for-Profit entities f. a self-service model of Data Entry of Rosters by employers, Academies, Security Guard Schools.
The Offerer's solution description must be provided below and on additional pages, if necessary:	
Solution Description:	
Evaluation Comments:	

Attachment 8

PSCTS Mandatory Base System Requirements - Solution and/or Documentation Descriptions with Forms Required for Vendor Bid Response

B. Records Management Solution/Documentation	
Item B.8	The current method for recording completion of security guard courses utilizes Optical Mark Reader (OMR) forms completed by the students and mailed to NYS by the school director. NYS staff utilizes a Pearson Op-Scan to collect the student data from the schools. The current system uses Object Linking and Embedding (OLE) technology to capture the underlying data. The data is then converted to a flat-file format for import into the Ingenium database and for daily export to NY Department of State (DOS). Describe how the system will allow for the processing of the data converted to a flat-file format for import into the database and for export to NY Department of State (DOS). The specific details of the current Security Guard Training process which includes the OMR data capture are depicted in a flowchart located in Appendix I.15, <i>Security Guard Training</i>.
The Offerer's solution description must be provided below and on additional pages, if necessary:	
Solution Description:	
Evaluation Comments:	

B. Records Management Solution/Documentation	
Item B.9	NYS approves Security Guard Instructor initial applications and subsequent recertification applications every five years. In addition, there are two categories of Security Guard Program Instructors; armed and unarmed. Each category requires specific pre-requisites. Proposed solution will provide a self-service model allowing Security Guard Instructors to submit initial applications as well as recertification applications every five years. Describe how the proposed solution will allow NYS to receive, review, and approve Security Guard Instructor applications. Include in the response how the system will: a. accommodate armed and unarmed Instructor applications b. allow prerequisites to be set for both armed and unarmed instructors c. assist with verifying pre-requisites for armed and unarmed instructors send automated notifications to instructors nearing or exceeding five year certification limits.
The Offerer's solution description must be provided below and on additional pages, if necessary:	
Solution Description:	
Evaluation Comments:	

Attachment 8

**PSCTS Mandatory Base System Requirements - Solution and/or Documentation Descriptions with Forms
Required for Vendor Bid Response**

B. Records Management Solution/Documentation	
Item B.10	The training history of each individual must follow that individual regardless of change in Employer(s), or name(s). These histories must be accessible to authorized persons requiring access to this information such as record holder(s), employers, and NYS. Describe how the proposed solution will; A. enable the training history of an officer, from recruit to retirement, to be recorded and accessible. B. enable training histories to follow each individual regardless of change in Employer(s), or name(s), or rank/title, and/or weapon indicator C. be capable of differentiating between weapons indicators for peace officers vs. police officers because the arming authority (or not) for peace officers may change from employer to employer D. be accessible to authorized persons requiring access to this information such as record holder(s), employers, and NYS.
The Offerer's solution description must be provided below and on additional pages, if necessary:	
Solution Description:	
Evaluation Comments:	

Attachment 8

PSCTS Mandatory Base System Requirements - Solution and/or Documentation Descriptions with Forms Required for Vendor Bid Response

C. Training Management Solution/Documentation	
Item C.1	Proposed solution shall allow NYS to manage on-line course registration and completion. Describe how the proposed system will; a. allow NYS to assign or customize pre-requisites for course enrollments. b. limit users ability to enroll in courses based on pre-requisites c. allow self-registration by users d. generate customized registration approval or disapproval notices based on pre-requisites. e. issue certificates upon course completion (include the format, e.g. Adobe@ PDF, MS WORD, etc) f. perform records management updates upon course completion Refer to Appendix K, Table 5, Learning Experiences, for a listing of current training courses and corresponding course pre-requisites.
The Offerer's solution description must be provided below and on additional pages, if necessary:	
Solution Description:	
Evaluation Comments:	

Attachment 8

PSCTS Mandatory Base System Requirements - Solution and/or Documentation Descriptions with Forms Required for Vendor Bid Response

D. Reports, Statistics & Audits Solution/Documentation	
Item D.1	NYS must have the ability to respond quickly and efficiently to all reporting requests, this includes requests for standard and ad-hoc information, without assistance from the vendor or need for advanced technical skill-set(s). The proposed system must allow NYS to create all standard reports, as described in Appendix K, Table 1 Report Requirements. Note: Offerer responses to items a, b, c and e below do not require a specific answer to each of the 28 reports listed in Appendix K, Table 1. The requirement is to address the proposed systems capability to produce the required reports and statistics. Any reports or statistics the system is incapable of producing must be listed in the response. Describe how the proposed solution will enable NYS to; a. respond quickly and efficiently to all standard reporting requests listed in Appendix K, Table 1. b. create ad-hoc <u>reports</u> on any single field or multiple fields including but not limited to all items listed in Appendix K, Table 1. c. generate standard and ad-hoc <u>statistics</u> on any single field or multiple fields including but not limited to all items listed in Appendix K, Table 1. d. obtain report information without assistance from the vendor or need for advanced technical skill-set(s). e. track and display month-to- month and year-to- year statistics for NYS staff work output that includes but is not limited to; 1) number of training courses approved 2) training courses completed 3) individual records updated 4) persons trained 5) certificates issued 6) Pistol Permit Verifications Completed (by New York State Police) 7) Freedom of Information Act requests completed 8) adhoc executive requests for reports 9) employer requests for records updates 10) individual requests for updates or transcripts, and instructors certified 11) the number of Registry transactions.
The Offerer's solution description must be provided below and on additional pages, if necessary:	
Solution Description:	
Evaluation Comments:	

Attachment 8

PSCTS Mandatory Base System Requirements - Solution and/or Documentation Descriptions with Forms Required for Vendor Bid Response

D. Reports, Statistics & Audits Solution/Documentation	
Item D.2	NYS requires a solution that will identify gaps in the validity and expiration of training certificates and identify gaps in an officer's service from one employer to another. When a Peace or Police officer leaves employment his or her Basic Course for Police Officer (BCPO) certificate will remain valid for various time periods established by law. The periods of certificate validity depend on the length of the officer's prior continuous employment. For example; if an officer completes BCPO training and serves less than two (2) years before leaving employment, the officer has two years to become reemployed or the certificate is deemed invalid and requires the officer to complete additional "refresher" training. Likewise, an officer that serves more than two (2) consecutive years would have four (4) years before his or her BCPO certificate will become invalid. Finally, an officer has ten (10) years from the last date employment to complete a refresher course or the BCPO certificate is expired. In this case, the officer would need to repeat the entire BCPO course. NYS requires a registry system that will identify and track gaps in training certificates such as the BCPO course as well as numerous other certifications that have expiration dates. The system must be capable of notifying NYS, employers and individual officers of existing gaps or the pending expirations of certifications. The system must contain a mechanism for NYS staff to provide final approval for any changes made by employers to resolve expired certificates. <i>Note:</i> Automated notifications associated with the audit requirements are a non-negotiable feature, details of logistics and /or procedure may be negotiable provided they are not cumbersome. Describe the audit capability of the proposed system and specifically address how the proposed system will: a. allow NYS to assign maturity, validity and/or expiration dates to certain certificates or qualifications. b. make automated notifications, as appropriate to NYS staff, employers, and individual officers for expiring or expired certificates. c. allow NYS staff to provide final approval for any changes made by employers to resolve expired certificates.
The Offerer's solution description must be provided below and on additional pages, if necessary:	
Solution Description:	
Evaluation Comments:	

Attachment 8

PSCTS Mandatory Base System Requirements - Solution and/or Documentation Descriptions with Forms Required for Vendor Bid Response

D. Reports, Statistics & Audits Solution/Documentation	
Item D.3	In order to manage compliance with training standards, NYS must be able to record, maintain and report on each officer's rank history, including transitions from one employer to another or from multiple employers and roles. This requirement coincides with the capability to provide gap analysis for validity of training certifications previously described in item 8.D.2. The proposed system must be able to record, maintain and report on each officer's rank history, including transitions from one employer to another or from multiple employers and roles. Describe how the system; a. accurately tracks rank history b. accurately employment history, and c. allows NYS to manage compliance with training standards associated with rank and employment histories.
The Offerer's solution description must be provided below and on additional pages, if necessary:	
Solution Description:	
Evaluation Comments:	

This Page Intentionally Blank

Attachment 9

Staffing Plan

Intentionally Blank

STAFFING PLAN

Submit with Bid or Proposal – Instructions on page 2

Solicitation No.:	Reporting Entity:	Report includes Contractor's/Subcontractor's: ☐ Work force to be utilized on this contract ☐ Total work force
Offeror's Name:	☐ Offeror ☐ Subcontractor	
Offeror's Address:	Subcontractor's name _____	

Enter the total number of employees for each classification in each of the EEO-Job Categories identified

EEO-Job Category	Work force by Gender		Work force by Race/Ethnic Identification					Work force by	
	Total Male (M)	Total Female (F)	White (M) (F)	Black (M) (F)	Hispanic (M) (F)	Asian (M) (F)	Native American (M) (F)	Disabled (M) (F)	Veteran (M) (F)
Officials/Administrators									
Professionals									
Technicians									
Sales Workers									
Office/Clerical									
Craft Workers									
Laborers									
Service Workers									
Temporary /Apprentices									
Totals									

PREPARED BY (Signature):	TELEPHONE NO.:	DATE:
NAME AND TITLE OF PREPARER (Print or Type):	EMAIL ADDRESS:	Submit completed with bid or proposal M/WBE 101 (Rev 11/08)

General instructions: All Offerors and each subcontractor identified in the bid or proposal must complete an EEO Staffing Plan (M/WBE 101) and submit it as part of the bid or proposal package. Where the work force to be utilized in the performance of the State contract can be separated out from the contractor's and/or subcontractor's total work force, the Offeror shall complete this form only for the anticipated work force to be utilized on the State contract. Where the work force to be utilized in the performance of the State contract cannot be separated out from the contractor's and/or subcontractor's total work force, the Offeror shall complete this form for the contractor's and/or subcontractor's total work force.

Instructions for completing:

- 1. Enter the Solicitation number that this report applies to along with the name and address of the Offeror.
- 2. Check off the appropriate box to indicate if the Offeror completing the report is the contractor or a subcontractor.
- 3. Check off the appropriate box to indicate work force to be utilized on the contract or the Offerors' total work force.
- 4. Enter the total work force by EEO job category.
- 5. Break down the anticipated total work force by gender and enter under the heading 'Work force by Gender'
- 6. Break down the anticipated total work force by race/ethnic identification and enter under the heading 'Work force by Race/Ethnic Identification'. Contact the OM/WBE Permissible contact(s) for the solicitation if you have any questions.
- 7. Enter information on disabled or veterans included in the anticipated work force under the appropriate headings.
- 8. Enter the name, title, phone number and email address for the person completing the form. Sign and date the form in the designated boxes.

RACE/ETHNIC IDENTIFICATION

Race/ethnic designations as used by the Equal Employment Opportunity Commission do not denote scientific definitions of anthropological origins. For the purposes of this form, an employee may be included in the group to which he or she appears to belong, identifies with, or is regarded in the community as belonging. However, no person should be counted in more than one race/ethnic group. The race/ethnic categories for this survey are:

- **WHITE** (Not of Hispanic origin) All persons having origins in any of the original peoples of Europe, North Africa, or the Middle East.
- **BLACK** a person, not of Hispanic origin, who has origins in any of the black racial groups of the original peoples of Africa.
- **HISPANIC** a person of Mexican, Puerto Rican, Cuban, Central or South American or other Spanish culture or origin, regardless of race.
- **ASIAN & PACIFIC ISLANDER** a person having origins in any of the original peoples of the Far East, Southeast Asia, the Indian subcontinent or the Pacific Islands.
- **NATIVE INDIAN (NATIVE AMERICAN/ ALASKAN NATIVE)** a person having origins in any of the original peoples of North America, and who maintains cultural identification through tribal affiliation or community recognition.

OTHER CATEGORIES

- **DISABLED INDIVIDUAL** any person who:
 - has a physical or mental impairment that substantially limits one or more major life activity(ies)
 - has a record of such an impairment; or
 - is regarded as having such an impairment.
- **VIETNAM ERA VETERAN** a veteran who served at any time between and including January 1, 1963 and May 7, 1975.
- **GENDER**

Male	or	Female

Attachment 10

MWBE Utilization Plan

Intentionally Blank

M/WBE UTILIZATION PLAN

INSTRUCTIONS: This form must be submitted with any bid, proposal, or proposed negotiated contract or within a reasonable time thereafter, but prior to contract award. This Utilization Plan must contain a detailed description of the supplies and/or services to be provided by each certified Minority and Women-owned Business Enterprise (M/WBE) under the contract. Attach additional sheets if necessary.

Offeror's Name:

Address:

City, State, Zip Code:

Telephone No.:

Region/Location of Work:

Federal Identification No.:

Solicitation No.:

Project No.:

M/WBE Goals in the Contract: MBE % WBE %

1. Certified M/WBE Subcontractors/Suppliers Name, Address, Email Address, Telephone No.	2. Classification	3. Federal ID No.	4. Detailed Description of Work (Attach additional sheets, if necessary)	5. Dollar Value of Subcontracts/ Supplies/Services and intended performance dates of each component of the contract.
A.	NYS ESD CERTIFIED ☐ MBE ☐ WBE			
B.	NYS ESD CERTIFIED ☐ MBE ☐ WBE			

6. IF UNABLE TO FULLY MEET THE MBE AND WBE GOALS SET FORTH IN THE CONTRACT, OFFEROR MUST SUBMIT A REQUEST FOR WAIVER FORM (M/WBE 104).

PREPARED BY (Signature): DATE:	TELEPHONE NO.:	EMAIL ADDRESS:
	FOR M/WBE USE ONLY	
	REVIEWED BY:	DATE:
NAME AND TITLE OF PREPARER (Print or Type): SUBMISSION OF THIS FORM CONSTITUTES THE OFFEROR'S ACKNOWLEDGEMENT AND AGREEMENT TO COMPLY WITH THE M/WBE REQUIREMENTS SET FORTH UNDER NYS EXECUTIVE LAW, ARTICLE 15-A, 5 NYCRR PART 143, AND THE ABOVE-REFERENCED SOLICITATION. FAILURE TO SUBMIT COMPLETE AND ACCURATE INFORMATION MAY RESULT IN A FINDING OF NONCOMPLIANCE AND POSSIBLE TERMINATION OF YOUR CONTRACT.		
UTILIZATION PLAN APPROVED: ☐ YES ☐ NO Date: _____ Contract No.: _____ Project No. (if applicable): _____ Contract Award Date: _____ Estimated Date of Completion: _____ Amount Obligated Under the Contract: _____ Description of Work: _____ NOTICE OF DEFICIENCY ISSUED: ☐ YES ☐ NO Date: _____ NOTICE OF ACCEPTANCE ISSUED: ☐ YES ☐ NO Date: _____		
M/WBE 103 (Revised 11/08)		

This Page Intentionally Blank

Attachment 11

Firm Offer Letter and Conflict of Interest Disclosure

Intentionally Blank

FIRM OFFER LETTER AND CONFLICT OF INTEREST DISCLOSURE
[TO BE COMPLETED ON OFFERER'S LETTERHEAD]

Date

Ms. Kimberly Szady
Director, Office of Financial Services
New York State Division of Criminal Justice Services
80 S. Swan Street, 10th Floor
Albany, New York 12210

Dear Ms. Szady:

RE: Public Safety Credentialing and Training System RFP CJS 2014 01
Firm Offer to the State of New York and Conflict of Interest Disclosure

[INSERT OFFERER NAME] hereby submits this firm and binding offer to the State of New York in response to New York State Request for Proposals (RFP) CJS 2014 01 by the New York State Division of Criminal Justice Services for the Peace Police Registry system . The Bid Proposal hereby submitted meets or exceeds all terms, conditions and requirements set forth in the above-referenced RFP. This formal offer will remain firm and non-revocable for a minimum period of one (1) year from the date proposals are due to be received by the State, or until a Contract is approved by the NYS Comptroller and executed by the State.

[INSERT OFFERER NAME]'s complete offer is set forth in two, separately bound volumes as follows:

Technical Proposal: Total of ____ hard copy volumes, with ____ electronic copies in _____ (disk, CD Rom) format.

Financial/Administrative Proposal: Total of ____ hard copy volumes, with ____ electronic copies in _____ (disk, CD Rom) format.

[INSERT OFFERER NAME] hereby affirms that the solution proposed by the Offerer in the Bid Proposal meets or exceeds the mandatory requirements set forth in RFP CJS 2014 01 including referenced attachments.

[INSERT OFFERER NAME] hereby affirms that, at the time of bid submission, Offerer knows of no factors existing at time of bid submission or which are anticipated to arise during the procurement or Contract term, which would constitute a potential conflict of interest in successfully meeting the contractual obligations set forth in the above-referenced RFP and the Bid Proposal hereby submitted, including but not limited to:

1. No potential for conflict of interest on the part of the Offerer or any Subcontractor due to prior, current, or proposed contracts, engagements, or affiliations; and
2. No potential conflicts in the sequence or timing of the proposed award under this procurement relative to the timeframe for service delivery, or personnel or financial resource commitments of Offerer or proposed subcontractors to other projects.

By signing, the undersigned individual affirms and represents that he has the legal authority and capacity to sign and make this offer on behalf of, and has signed using that authority to legally bind **[INSERT OFFERER NAME]** to the offer, and possesses the legal capacity to act on behalf of Offerer to execute a Contract with the State of New York. The aforementioned legal authority and capacity of the undersigned individual is affirmed by the enclosed Resolution of the Corporate Board of Directors of **[INSERT OFFERER NAME]**.

Signature
[INSERT OFFERER NAME]
[INSERT TITLE]
[INSERT COMPANY NAME]

Corporate Seal, if applicable

CORPORATE ACKNOWLEDGMENT

STATE OF	}	
	:ss.:	
COUNTY OF	}	
On the _____ day of _____ in the year 201 __ , before me personally came: _____, to me known, who, being by me duly sworn, did depose and say that he/she/they reside(s) in _____; that he/she/they is (are) _____ (the President or other officer or director or attorney in fact duly appointed) of _____, the corporation described in and which executed the above instrument; and that he/she/they signed his/her/their name(s) thereto by authority of the board of directors of said corporation.		
Signature and Office of Person Taking Acknowledgment		

PARTNERSHIP ACKNOWLEDGMENT

STATE OF	}	
	:ss.:	
COUNTY OF	}	
On the _____ day of _____ in the year 201 __, before me personally came: _____ to me known, who, being by me duly sworn, did depose and say that he reside(s) in _____; that he is _____ (the General/Managing Partner or other officer or attorney in fact duly appointed) of _____, the partnership described in said instrument; that, by the terms of said partnership, he is authorized to execute the foregoing instrument on behalf of the partnership for the purposes set forth therein; and that, pursuant to that authority, he executed the foregoing instrument in the name and on behalf of said partnership as the act and deed of said partnership.		
Signature and Office of Person Taking Acknowledgment		

INDIVIDUAL ACKNOWLEDGEMENT

STATE OF	}	
	:ss.:	
COUNTY OF	}	
On the ____ day of _____ in the year 201 __ , before me personally appeared: _____, known to me to be the person who executed the foregoing instrument, who, being duly sworn by me did depose and say that he resides at _____, Town of _____, County of _____, State of _____; and that he executed the foregoing instrument in his/her name and on his/her own behalf.		
Notary Public		

This Page Intentionally Blank

Attachment 12

Non-Discrimination in Employment in Northern Ireland Statement

Intentionally Blank

Non-Discrimination in Employment in Northern Ireland Statement

State Finance Law §165 requires that before entering into certain State contracts, persons or entities must certify that they either have no business operations in Northern Ireland or that such business operations will be conducted in accordance with the MacBride Fair Employment Principles. Please answer the following questions and return form with your bid or contract.

1. Does the Offerer or any individual or legal entity in which the Offerer holds a 10 percent or greater ownership interest, or any individual or legal entity that holds a 10 percent or greater ownership interest in the Offerer, have any business operations in Northern Ireland?

No ☐ Yes ☐

2. If yes, does the Offerer certify that it shall take lawful steps in good faith to conduct any business operations they have in Northern Ireland in accordance with the MacBride Fair Employment Principles, relating to nondiscrimination in employment and freedom of workplace opportunity regarding such operations in Northern Ireland, and that it shall permit independent monitoring of their compliance with such Principles?

No ☐ Yes ☐

By: _____
Signature of Authorized Representative

Name (Please print)

Title (Please print)

Offerer

Date

Attachment 13

Non-Collusive Bidding Certification

Intentionally Blank

NON-COLLUSIVE BIDDING CERTIFICATION REQUIRED BY
SECTION 139-D OF THE STATE FINANCE LAW

SECTION 139-D, Statement of Non-Collusion in bids to the State:

BY SUBMISSION OF THIS BID, BIDDER AND EACH PERSON SIGNING ON BEHALF OF BIDDER CERTIFIES, AND IN THE CASE OF JOINT BID, EACH PARTY THERETO CERTIFIES AS TO ITS OWN ORGANIZATION, UNDER PENALTY OF PERJURY, THAT TO THE BEST OF HIS/HER KNOWLEDGE AND BELIEF:

[1] The prices of this bid have been arrived at independently, without collusion, consultation, communication, or agreement, for the purposes of restricting competition, as to any matter relating to such prices with any other Bidder or with any competitor;

[2] Unless otherwise required by law, the prices which have been quoted in this bid have not been knowingly disclosed by the Bidder and will not knowingly be disclosed by the Bidder prior to opening, directly or indirectly, to any other Bidder or to any competitor; and

[3] No attempt has been made or will be made by the Bidder to induce any other person, partnership or corporation to submit or not to submit a bid for the purpose of restricting competition.

A BID SHALL NOT BE CONSIDERED FOR AWARD NOR SHALL ANY AWARD BE MADE WHERE [1], [2], [3] ABOVE HAVE NOT BEEN COMPLIED WITH; PROVIDED HOWEVER, THAT IF IN ANY CASE THE BIDDER(S) CANNOT MAKE THE FOREGOING CERTIFICATION, THE BIDDER SHALL SO STATE AND SHALL FURNISH BELOW A SIGNED STATEMENT WHICH SETS FORTH IN DETAIL THE REASONS THEREFORE:

Non-Collusive Bidding Certification-1

[AFFIX ADDENDUM TO THIS PAGE IF SPACE IS REQUIRED FOR STATEMENT.]

Subscribed to under penalty of perjury under the laws of the State of New York, this _____ day of _____, 20____ as the act and deed of said corporation or partnership.

IF BIDDER(S) (ARE) A PARTNERSHIP, COMPLETE THE FOLLOWING:

NAMES OF PARTNERS OR PRINCIPALS

LEGAL RESIDENCE

President:

Secretary:

Treasurer:

President:

Secretary:

Treasurer:

Joint or combined bids by companies or firms must be certified on behalf of each participant.

Potential Contractor(s): _____

Name: _____
If applicable, responsible corporate officer

Title: _____

Address: _____

Telephone: _____

Potential Contractor(s): _____

Name: _____
If applicable, responsible corporate officer

Title: _____

Address: _____

Telephone: _____

Attachment 14

Prohibitions on Procurement Lobbying

Intentionally Blank

Division of Criminal Justice Services
Summary of Policy and Prohibitions on Procurement Lobbying

Background:

State Finance Law §139-j(6) requires that a Governmental Entity incorporate a summary of its policy and prohibitions regarding permissible Contacts during a covered procurement.

Pursuant to State Finance Law §§139-j and 139-k, this solicitation includes and imposes certain restrictions on communications between a Governmental Entity and an Offerer/bidder during the procurement process. An Offerer/bidder is restricted from making contacts from the earliest notice of intent to solicit offers through final award and approval of the Procurement Contract by the Governmental Entity and, if applicable, Office of the State Comptroller (“restricted period”) to other than designated staff unless it is a contact that is included among certain statutory exceptions set forth in State Finance Law §139-j (3)(a). Designated staff, as of the date hereof, is identified on the first page of this solicitation. DCJS employees are also required to obtain certain information when contacted during the restricted period and make a determination of the responsibility of the Offerer/bidder pursuant to these two statutes. Certain findings of non-responsibility can result in rejection for contract award and in the event of two findings within a 4 year period, the Offerer/bidder is debarred from obtaining governmental Procurement Contracts. Further information about these requirements can be found at the OGS website:

<http://www.ogs.state.ny.us/aboutOgs/regulations/defaultAdvisoryCouncil.html>

Mandatory Submissions:

The Division of Criminal Justice Services’ Procurement Lobbying Guidelines are attached. The Offerer/Bidder must affirm that it understands and agrees to comply with DCJS’ procedures relative to the State Finance Law § 139-j (3) and § 139-j (6) (b) by completing and submitting Attachment 1 to the DCJS Procurement Lobbying Guidelines.

The Offerer/Bidder must also complete and submit Attachment 2 to the DCJS Procurement Lobbying Guidelines, the “Offerer Disclosure of Prior Non-Responsibility Determinations” and Form 4, “Offerer’s Certification of Compliance with State Finance Law §139-k (5).

DIVISION OF CRIMINAL JUSTICE SERVICES PROCUREMENT LOBBYING GUIDELINES

I. INTRODUCTION

These Guidelines, which have been issued pursuant to the New York State Finance Law, apply to all Division of Criminal Justice Services' ("DCJS") procurement contracts and limit certain types of communications between Offerers and DCJS during the Restricted Period of a Governmental Procurement. During the Restricted Period, an Offerer may communicate only with the person or persons designated by DCJS to receive communications regarding such Governmental Procurement.

II. STATUTORY DEFINITIONS

Article of Procurement	A commodity, service, technology, public work, construction, revenue contract, or the purchase, sale or lease of real property or an acquisition or granting of an interest in real property that is the subject of a governmental procurement.
Contact	Any oral, written or electronic communication with DCJS under circumstances where a reasonable person would infer that the communication was intended to influence the governmental procurement.
Governmental Entity	Includes New York State agencies, public benefit corporations, public authorities of which at least one member is appointed by the Governor, both houses of the New York State Assembly and Senate, the Unified Court System, and certain Industrial Development Agencies.
Governmental Procurement	(i) the preparation of terms of the specifications, bid documents, requests for proposals, or evaluations criteria for a procurement contract, (ii) solicitation for a procurement contract, (iii) evaluation of a procurement contract, (iv) award, approval, denial or disapproval of a procurement contract, or (v) approval or denial of an assignment, amendment (other than amendments that are authorized and payable under the terms of the procurement contract as it was finally awarded or approved by the Comptroller, as applicable), renewal or extension of a procurement contract, or any other material change in the procurement contract resulting in a financial benefit to the Offerer.

Offerer	The individual or entity, or any employee agent or consultant or person acting on behalf of such individual or entity, that contacts DCJS about a Governmental Procurement .
Procurement Contract	Any contract or other agreement for an Article of Procurement involving an estimated annualized expenditure in excess of \$15,000. Grants, Article Eleven-B State Finance Law Contracts, Intergovernmental Agreements, Railroad and Utility Force Accounts, Utility Relocation Project Agreements or Orders of Eminent Domain Transactions shall not be deemed Procurement Contracts in these Guidelines.
Restricted Period	The period of time commencing with the earliest date of written notice, advertisement or solicitation of a request for proposal, invitation for bids, or solicitation of proposals, or any other method for soliciting a response from Offerers intending to result in a Procurement Contract with DCJS and, ending with the final contract award and approval by, where applicable, the Office of the State Comptroller.

III. EXEMPTIONS

While an **Offerer** shall only contact the person or persons who may be contacted by **Offerers** as designated by the governmental entity relative to the government procurement during the restricted period, certain communications are exempt from these Guidelines. These include: (i) submissions in response to an invitation for bid, a request for proposal or other solicitation, (ii) submissions of written questions to a designated contact set forth in an invitation for bid, request for proposal or other solicitation, (iii) participation in a conference provided for in an invitation for bid, request for proposal or other solicitation, (iv) contract negotiations, (v) inquiries regarding the factual status of a **Procurement Contract**, and (vi) complaints and protests regarding the procurement process and outcome.

IV. NEW YORK STATE LEGISLATURE OR LEGISLATIVE STAFF

Any communication received by DCJS from members of the New York State Legislature or legislative staff, when acting in their official capacity, shall not be considered a **Contact**.

V. VIOLATIONS

A violation of these Guidelines occurs when there is a **Contact** during the **Restricted Period** between the **Offerer** and someone other than the person or persons designated by DCJS to receive communications for the particular **Governmental Procurement**. This includes instances where the **Offerer Contacts** DCJS regarding **Governmental Procurements** of other **Governmental Entities**.

Attempts by an **Offerer** to influence a **Governmental Procurement** in a manner that would result in a violation of the Public Officers Law or Penal Law also shall also be a violation of these Guidelines.

VI. PROCEDURES

A. Notifying Vendors of Procurement Lobbying Guidelines

1. For each **Procurement Contract**, the DCJS Finance Office will designate a person or persons to receive communications from **Offerers** concerning the **Procurement Contract**.
2. The DCJS Finance Office will incorporate a summary of the policy and prohibitions regarding permissible communications during a **Governmental Procurement** in its documents relating to the **Procurement Contract** and provide a copy of these Guidelines in such documents.
3. The DCJS Finance Office shall seek written affirmation from all **Offerers** as to the **Offerer's** understanding of and agreement to comply with these Guidelines (Attachment 1).

B. Making Determinations of Responsibility

1. Prior to award of a **Procurement Contract**, DCJS must make a responsibility determination with respect to the **Offerer** to be recommended for the award of the contract based upon, among other things, the information supplied by that **Offerer**. The **Offerer** must disclose, using the **Offerer** Disclosure of Prior Non-Responsibility Determinations Form (Attachment 2), whether it has been found non-responsible within the last four years by any **Governmental Entity** for: (1) failure to comply with State Finance Law §139-j; or (2) the intentional provision of false, inaccurate or incomplete information. This disclosure must be certified by the **Offerer** and must affirmatively state that the information supplied by the **Offerer** to DCJS is complete, true and accurate.
2. Any **Procurement Contract** award shall contain a certification by the **Offerer** that all information provided to DCJS is complete, true and accurate. Each DCJS contract shall contain a provision authorizing DCJS to terminate the contract in the event the certification is found to be intentionally false, intentionally incomplete, or intentionally inaccurate. DCJS will include in the procurement record a statement describing the basis for any action taken pursuant to such termination provision. Admissions by the **Offerer** of past findings of non-responsibility may constitute a basis for rejection of the **Offerer** by DCJS. DCJS shall include in the procurement record a statement describing the basis for any action taken pursuant to such termination provision. DCJS can award a contract to the **Offerer** despite the past findings of non-responsibility if it determines that the award of the **Procurement Contract** to the **Offerer** is necessary to protect public property or public health or safety, and that the **Offerer** is the only source capable of supplying the required **Articles of Procurement** within the necessary time frame. The basis of such a finding must be included in the procurement record of the **Procurement Contract**.

C. Recording of **Contacts**

1. All DCJS employees must record any **Contact**. As defined, a **Contact** is one from any person or entity that is intended to influence procurement. However, any communication received by DCJS from members of the New York State Legislature, or the Legislative Staffs, when acting in their official capacity, shall not be recorded.
2. Upon any **Contact** during the restricted period, DCJS shall obtain the name, address, telephone number, place of principal employment and occupation of the person or organization making the contact and inquire and record whether the person or organization making such contact was the **Offerer** or was retained, employed or designated by or on behalf of the offerer to appear before or contact DCJS about the governmental procurement. **Contact** may be initiated by parties with an interest in the procurement that are not necessarily connected directly to the **Offerer**. **Contact** may come in the form of telephone conversations, correspondence, electronic mail and person-to-person discussions. The Record of Procurement Contact Form (Attachment 3) should be used to record **Contacts**. The form is available on the DCJS Intranet homepage under “Policies and Procedures,” “Record of Procurement Contact.” The form should be completed by the DCJS employee and e-mailed to “dcjsProcurementlaw@dcjs.ny.gov,” an e-mail account on the DCJS internal e-mail system. This e-mail account will send the form to both the DCJS Finance Office and the DCJS Ethics Officer.
3. The exempted communications set forth in Article III need not be reported unless a reasonable person would infer that the communications were intended to influence the procurement.
4. If a DCJS employee is in doubt about whether a communication was intended to influence the **Governmental Procurement**, he or she should record the communication on the Record of Procurement Contact Form and submit it to dcjsProcurementlaw@dcjs.ny.gov for further investigation.
5. The DCJS Finance Office will be required to include all Records of Procurement Contact in the procurement record for the related **Procurement Contract**.

D. Investigation of Contacts/ Penalties for Violations

1. All reported Contacts will be immediately investigated by the DCJS Ethics Officer, or his or her designee. If the DCJS Ethics Officer finds sufficient cause to believe that an Offerer has violated these Guidelines, the Offerer will be notified in writing of the investigation and will be afforded an opportunity to respond to the alleged violation. Investigations will be completed as soon as practicable so as not to delay the progress of the Governmental Procurement.

2. If the DCJS Ethics Officer should find at the conclusion of the investigation that the Offerer knowingly and willfully made prohibited Contact in violation of these Guidelines, then the Offerer shall be disqualified as non-responsible, unless DCJS makes a finding that the award of the Procurement Contract to the Offerer is necessary to protect public property or public health or safety, and that the Offerer is the only source capable of supplying the required Article of Procurement within the necessary time frame. The basis of such a finding must be included in the procurement record of the Procurement Contract.

Form 1

Offerer's Affirmation of Understanding of and Agreement pursuant to State Finance Law §139-j (3) and §139-j (6) (b)

Background:

State Finance Law §139-j(6)(b) provides that:

Every Governmental Entity shall seek written affirmations from all Offerers as to the Offerer's understanding of and agreement to comply with the Governmental Entity's procedures relating to permissible contacts during a Governmental Procurement pursuant to subdivision three of this section.

Instructions:

A Governmental Entity must obtain the required affirmation of understanding and agreement to comply with procedures on procurement lobbying restrictions regarding permissible Contacts during the restricted period for a procurement contract in accordance with State Finance Law §§139-j and 139-k. This affirmation shall be obtained as early as possible in the procurement process, such as when the Offerer submits its proposal or bid.

I hereby affirm that I have read, understand and agree to comply with the Division of Criminal Justice Services' procedures related to permissible Contacts during a Governmental Procurement as required by State Finance Law §139-j (3) and §139-j (6) (b).

By: _____ Date: _____

Name: _____ (Please print)

Title: _____

Offerer Name: _____

Offerer Address: _____

Form 2

Offerer Disclosure of Prior Non-Responsibility Determinations

Background:

New York State Finance Law §139-k (2) obligates a Governmental Entity to obtain specific information regarding prior non-responsibility determinations with respect to State Finance Law §139-j. This information must be collected in addition to the information that is separately obtained pursuant to State Finance Law §163(9). In accordance with State Finance Law §139-k, an Offerer must be asked to disclose whether there has been a finding of non-responsibility made within the previous four (4) years by any Governmental Entity due to: (a) a violation of State Finance Law §139-j or (b) the intentional provision of false or incomplete information to a Governmental Entity. The terms “Offerer” and “Governmental Entity” are defined in State Finance Law § 139-k(1). State Finance Law §139-j sets forth detailed requirements about the restrictions on Contacts during the procurement process. A violation of State Finance Law §139-j includes, but is not limited to, an impermissible Contact during the restricted period (for example, contacting a person or entity other than the designated contact person, when such Contact does not fall within one of the exemptions).

As part of its responsibility determination, State Finance Law §139-k(3) mandates consideration of whether an Offerer fails to timely disclose accurate or complete information regarding the above non-responsibility determination. In accordance with law, no Procurement Contract shall be awarded to any Offerer that fails to timely disclose accurate or complete information under this section, unless a finding is made that the award of the Procurement Contract to the Offerer is necessary to protect public property or public health safety, and that the Offerer is the only source capable of supplying the required Article of Procurement within the necessary timeframe. See State Finance Law §§139-j (10)(b) and 139-k(3).

Instructions:

A Governmental Entity must include a disclosure request regarding prior non-responsibility determinations in accordance with State Finance Law §139-k in its solicitation of proposals or bid documents or specifications or contract documents, as applicable, for procurement contracts. The attached form is to be completed and submitted by the individual or entity seeking to enter into a Procurement Contract. It shall be submitted to the Governmental Entity conducting the Governmental Procurement.

As an alternative to this form, the Governmental Entity may elect to incorporate this disclosure question into its procurement questionnaire, such as the New York State Standard Vendor Responsibility Questionnaire set out at <http://www.ogs.state.ny.us/procurecounc/pdfdoc/BestPractice.pdf>

Offerer Disclosure of Prior Non-Responsibility Determinations

Name of Individual or Entity Seeking to Enter into the Procurement Contract:

Address: _____

Name and Title of Person Submitting this Form: _____

Contract Procurement Number: _____

Date: _____

1. Has any Governmental Entity made a finding of non-responsibility regarding the individual or entity seeking to enter into the Procurement Contract in the previous four years? (Please circle):

No

Yes

If yes, please answer the next questions:

2. Was the basis for the finding of non-responsibility due to a violation of State Finance Law §139-j (Please circle):

No

Yes

3. Was the basis for the finding of non-responsibility due to the intentional provision of false or incomplete information to a Governmental Entity? (Please circle):

No

Yes

4. If you answered yes to any of the above questions, please provide details regarding the finding of non-responsibility below.

Governmental Entity:

Date of Finding of Non-responsibility:

Basis of Finding of Non-Responsibility: _____

(Add additional pages as necessary)

5. Has any Governmental Entity or other governmental agency terminated or withheld a Procurement Contract with the above-named individual or entity due to the intentional provision of false or incomplete information? (Please circle):

No

Yes

6. If yes, please provide details below.

Governmental Entity: _____

Date of Termination or Withholding of Contract:

Basis of Termination or Withholding: _____

(Add additional pages as necessary)

Offerer certifies that all information provided to the Governmental Entity with respect to State Finance Law §139-k is complete, true and accurate.

By: _____ Date: _____

Signature

Name: _____

Title: _____

FORM 3

**Offerer's Certification of Compliance
With State Finance Law §139-k(5)**

Background:

New York State Finance Law §139-k(5) requires that every Procurement Contract award subject to the provisions of State Finance Law §§139-k or 139-j shall contain a certification by the Offerer that all information provided to the procuring Governmental Entity with respect to State Finance Law §139-k is complete, true and accurate.

Instructions:

A Governmental Entity must obtain the required certification that the information is complete, true and accurate regarding any prior findings of non-responsibility, such as non-responsibility pursuant to State Finance Law §139-j. The Offerer must agree to the certification and provide it to the procuring Governmental Entity

The Offerer/Bidder shall submit the following certification with its bid.

Offerer Certification:

I certify that all information provided to the Governmental Entity with respect to State Finance Law §139-k is complete, true and accurate.

By: _____ Date: _____

Name: _____

Title: _____

Offerer's Name:

Offerer's Address:

This Page Intentionally Blank

Attachment 15

Tax Law

Intentionally Blank

**Questions and Answers
Concerning
Tax Law Section 5-a
(as amended, effective April 26, 2006)**

**Contractor, Affiliate and
Subcontractor Sales and
Compensating Use Tax
Certification**

Note: Although accurate, some of the definitions given in this publication have been simplified. If there is any discrepancy between the definitions of the terms in this publication and applicable New York law or regulations, then the law and regulations will govern.

1) **Q:** What does Tax Law section 5-a require?

A: The statute requires certain contractors awarded certain state contracts valued at more than \$100,000 to certify to the Tax Department that they are registered to collect New York State and local sales and compensating use taxes, if they made sales delivered by any means to locations within New York State of tangible personal property or taxable services having a cumulative value in excess of \$300,000, measured over a specified period. In addition, contractors must certify to the Tax Department that each affiliate and subcontractor of such contractor exceeding such sales threshold during a specified period is registered to collect New York State and local sales and compensating use taxes. Contractors must also certify to the procuring state entity that they filed the certification with the Tax Department and that it is correct and complete.

2) **Q:** What is the purpose of section 5-a?

A: The statute's aim is to ensure that contractors do not get state work unless they, their affiliates and their subcontractors are, when required by section 5-a, registered to collect New York State and local sales and compensating use taxes. Included within the statute's scope are out-of-state businesses making sales of more than \$300,000 into New York but having no physical presence in the state. Other businesses, if affiliated with, or subcontractors of, a bidder for a state contract, would similarly have to consent to registration as a condition of the contractor's obtaining state work, providing the affiliate's or subcontractor's sales exceed the \$300,000 sales threshold.

3) **Q:** Under what circumstances does section 5-a apply?

A: A contract is covered by section 5-a if:

- i. The procuring entity is a *covered agency* within the meaning of the statute (see Q & A 5);
- ii. The contractor is a *contractor* within the meaning of the statute (see Q & A 6); and
- iii. The contract is a *contract* within the meaning of the statute. This is the case when it (a) has a value in excess of \$100,000, and (b) is a contract for *commodities* or *services*, as such terms are defined for purposes of the statute (see Q & A 8 and 9). Furthermore, the procuring entity must have begun the solicitation to purchase on or after January 1, 2005, and the resulting contract must have been awarded, amended, extended, renewed, or assigned *on or after April 26, 2006* (the effective date of the section 5-a amendments).

If all of the above criteria are met, amended section 5-a is applicable and, as general matter, two certifications (Forms ST-220-CA and ST-220-TD) are required to be filed. These forms are available at www.nystax.gov.

If any of the above criteria are not met, amended section 5-a is not applicable and no certifications (no forms) are required to be filed.

4) **Q:** Are any contracts expressly exempted from application of section 5-a?

A: Yes. A contract will be exempted from application of section 5-a if the procuring covered agency and OSC, or other contract reviewer if OSC is not required to approve the contract, find in writing that the contract is necessary to:

- (a) address an emergency, within the meaning of Article 11 of the State Finance Law¹; or
- (b) ensure the public health, safety, or welfare when an urgent event with a compelling public purpose arises.

In addition, the agency's and contract reviewer's written finding must explain the reasons supporting the determination.

5) **Q:** What governmental entities are *covered agencies* for purposes of Tax Law section 5-a?

A: Tax Law section 5-a defines a *covered agency* to mean:

- a *state agency* for purposes of Article 11 of the New York State Finance Law; or
- a public authority or public benefit corporation at least one of whose members is appointed by the Governor.

For purposes of Article 11 of the New York State Finance Law, the term *state agency* includes all state departments, boards, commissions, offices or institutions. As such, the Department of Law, Office of the State Comptroller and the Education Department are included. Local government entities are **not** covered agencies for purposes of section 5-a.

¹ An *emergency* within the meaning of the State Finance Law is "an urgent and unexpected requirement where health and public safety or the conservation of public resources is at risk."

6) **Q:** Who is a *contractor* for purposes of section 5-a?

A: The statute defines a *contractor* as a person awarded a contract by a covered agency. The term *person* is defined as an individual, partnership, limited liability company, society, association, joint stock company or corporation.

The term *person* does **not** include a public corporation or an education corporation, as such terms are defined in section 66 of the New York State General Construction Law, a not-for-profit corporation whose contracts are subject to approval in accordance with Article 11-B of the New York State Finance Law, a board of cooperative educational services created pursuant to Article 40 of the New York State Education Law, or a soil and water conservation district created pursuant to section 5 of the New York State Soil and Water Conservation Districts Law.

As defined in the New York State General Construction Law:

- The term *public corporation* includes a municipal corporation, a district corporation and a public benefit corporation.
- A *municipal corporation* includes a county, city, town, village and school district.
- A *district corporation* includes any territorial division of the state, other than a municipal corporation, established by law, which possesses the power to contract indebtedness and levy taxes or benefit assessments upon real estate or to require the levy of such taxes or assessments, whether or not such territorial division is expressly declared to be a body corporate and politic by the statute creating or authorizing the creation of such territorial division.
- A *public benefit corporation* is a corporation organized to construct or operate a public improvement wholly or partly within the state, the profits from which inure to the benefit of New York State or other states, or to the people thereof.
- As defined in the New York State General Construction Law and the New York State Education Law, the term *education corporation* means a corporation
 - chartered or incorporated by the Board of Regents of the University of the State of New York or otherwise formed under the New York State Education Law, or
 - formed by a special act of New York State with its principal purpose an education purpose and which is a member of the University of the State of New York, or
 - formed under laws other than the statutes of New York State which, if it were to be formed currently under the laws of New York State, might be chartered by the Board of Regents of the University of the State of New York, and which has been authorized to conduct its activities in this state by the Regents or as an authorized foreign education corporation with the consent of the New York State Commissioner of Education.

7) **Q:** When does award of a contract occur for purposes of section 5-a?

A: A contract is awarded when the procuring covered agency notifies a person either orally or in writing that the person has been selected to provide the commodities or perform the services being procured. The certifications required by section 5-a are only required to be filed by the person awarded a contract.

8) **Q:** What contracts let by covered agencies are subject to section 5-a?

A: The statute defines the term *contract* as an agreement between a contractor and a covered agency for the purchase by the covered agency, pursuant to Article 11 of the New York State Finance Law, of commodities or services having a value in excess of \$100,000. The statute also expressly includes within the definition of *contract* centralized contracts with values in excess of \$100,000.

The definition of *contract* in section 5-a is broad enough to include, but is not limited to, the following types of contracts:

- backdrop contracts;
- single source contracts;
- sole source contracts;
- multiple award contracts;
- piggybacking contracts;
- strategic partnership procurement contracts; and
- contracts for the state.

Definitions

The term *commodities* has the meaning given by Article 11 of the New York State Finance Law, and includes (other than with respect to contracts for state printing) material goods, supplies, products, construction items, or other standard articles of commerce, other than technology, which are the subject of any purchase or other exchange.

The term *services* has the meaning given by Article 11 of the New York State Finance Law. *Services* means (other than with respect to contracts for state printing) the performance of a task or tasks, and may include a material good or a quantity of material goods, and which is the subject of any purchase or other exchange. For Article 11 purposes, *services* includes technology.² The term *services* does **not** apply to contracts for architectural, engineering or surveying services, or to contracts with not-for-profit organizations approved in accordance with Article 11-B of the New York State Finance Law.

9) Q: Is a contract for information technology (IT) services subject to Tax Law Section 5-a?

A: Yes, assuming the criteria identified in Q & A 3 are met. When an IT service contract is awarded to a contractor, the section 5-a certifications must be made on Forms ST-220-CA and ST-220-TD irrespective as to whether the contractor is providing (1) only custom software, (2) only hardware and pre written off-the-shelf software, or (3) a combination of (1) and (2).

On Form ST-220-TD, a certification is made by the contractor as to whether the contractor, an affiliate(s) and/or subcontractor(s) made sales in New York State of *tangible personal property* (TPP) or *taxable services*, as set forth under the Tax Law, that exceeded \$300,000 over a certain look-back test period. If such sales threshold is met, then a certification is made that the contractor, affiliate(s) and/or subcontractor(s) is (are) registered to collect sales tax in New York. If the threshold is not met, then the contractor marks the box on Form ST-220-TD indicating that fact.

Pre written computer software (including software delivered electronically) and computer hardware constitute TPP for sales tax purposes, and therefore, are counted towards the \$300,000 New York sales threshold. In contrast, custom software (which is computer software designed to the specifications of a specific purchaser) is **neither** TPP nor a taxable service. Thus, the amount of sales derived from custom software is **not** counted towards this \$300,000 sales tax threshold.

Example:

*A contractor made sales in New York State valued at \$1,000,000 during the test period specified in section 5-a of **only** custom software, which is neither TPP nor a taxable service. Under such circumstances the contractor would certify on Form ST-220-TD that it did **not** meet the \$300,000 sales threshold by marking the bottom box in Section 1 of the form. Although total sales exceeded \$300,000, custom software does not fit the criteria of being TPP or taxable services and cannot be counted toward the \$300,000 sales threshold.*

However, if the contractor also made sales of pre-written computer software (TPP) in the amount of \$500,000 during the same look-back test period, then the contractor must certify that it was registered to collect sales tax in New York. Accordingly, the contractor must mark the first box in Section 1 on Form ST-220-TD.

Under both scenarios above, the contractor must also certify to the procuring agency on Form ST-220-CA that it also filed Form ST-220-TD with the Tax Department.

10) Q: What contract types are excluded from the definition of *contract* under section 5-a?

A: The following are not included within the definition of *contract* in section 5-a:

- contracts based on formal mini-bid solicitations pursuant to centralized contracts;
- grants;
- revenue contracts;
- intergovernmental agreements; and
- contracts with preferred sources as defined in Article 11 of the New York State Finance Law.

11) Q: Is the more than \$100,000 threshold determined based on total contract value, or on an annualized basis?

A: The more than \$100,000 threshold is determined based on the value (estimated, if necessary) of the contract over its full term, excluding possible renewal terms.

Also, multiple purchases of commodities or services by a covered agency from the same contractor during a state fiscal year are not to be aggregated for purposes of determining whether the more than \$100,000 threshold has been met.

² The term *technology* is defined by Article 11 of the New York State Finance Law as either a good or a service or a combination of the two, that results in a technical method of achieving a practical purpose or in improvements in productivity. Goods may be either new or used.

12) Q: If a contract is not let pursuant to Article 11 of the State Finance Law, is it subject to section 5-a?

A: Contracts not let pursuant to Article 11 of the State Finance Law are **not** subject to section 5-a.

13) Q: Does Tax Law section 5-a apply to an agency accessing a centralized contract through issuance of a purchase order?

A: Assuming all criteria identified in Q&A 3 are met, Tax Law section 5-a applies to award of the centralized contract and not to covered agency access to the centralized contract through issuance of a purchase order. However, the requirements of Tax Law section 5-a do apply to covered agency purchases using **all-copy purchase orders**. For information regarding all-copy purchase orders, contact the Office of the State Comptroller, Bureau of Contracts at (518) 474-4622.

14) Q: Is a mini-bid contract, which is let by a covered agency from a backdrop contract, subject to Tax Law Section 5-a?

A: No. A backdrop contract is one in which a procuring agency selects a pool of qualified vendors that are deemed eligible to bid on a procurement via a mini-bid. A mini-bid is an abbreviated process during which contract users solicit final pricing from the pool of pre-selected back-drop contractors.

A state agency backdrop procurement is deemed awarded to a contractor at the point in time when the vendor is selected to be included in the pool of contractors eligible to participate in a mini-bid process. In view of that, a contractor is required to submit the Tax Law section 5-a forms when selected as a backdrop vendor by a state agency. During a mini-bid process, additional section 5-a certifications by a backdrop contractor are not required unless there are changes necessitating a new filing. For instance, if during a mini bid, a contractor hires a new subcontractor which was not previously reported on its Form ST-220-TD, then the contractor should report the new subcontractor by filing of a new Form ST-220-TD (assuming the subcontractor meets the more than \$300,000 sales in New York State threshold).

15) Q: Who is an *affiliate* for purposes of Tax Law section 5-a?

A: Section 5-a defines an *affiliate* as a person which directly, indirectly or constructively controls another person; is controlled by another person; or is, along with another person, under the control of a common parent. *Control* means possession of the power to direct, or cause the direction of, the management and policies of another person. Determining whether control exists is a factual inquiry to be based upon the circumstances in each case. Responsibility for determining whether a person is an affiliate rests with the contractor.

16) Q: Who is a *subcontractor* for purposes of Tax Law section 5-a?

A: A *subcontractor* is a person engaged by a contractor or another subcontractor to perform a portion of the contractor's obligations under a contract.

17) Q: Which contractors, affiliates and subcontractors must be certified as registered to collect New York State and local sales and compensating use taxes pursuant to section 5-a prior to a contract taking effect?

A: Those contractors, affiliates and subcontractors making sales delivered by any means to locations within New York State of tangible personal property or taxable services having a value in excess of \$300,000 during a specified period must be certified as registered to collect New York State and local sales and compensating use taxes.

All sales of tangible personal property or taxable services within New York State during the specified period (not merely sales to covered agencies) are taken into account in determining whether the more than \$300,000 cumulative sales threshold has been met. This also includes the amount of any sales made which are exempt from sales tax (see Q & A 20).

18) Q: Over what period must the more than \$300,000 cumulative sales threshold occur so as to require a contractor, affiliate, or subcontractor to be certified under Tax Law section 5-a as registered with the Tax Department to collect sales and compensating use taxes?

A: The registration requirement applies if the person made a cumulative total of more than \$300,000 in sales in New York State during the four completed sales tax quarters which immediately precede the sales tax quarter in which the certification is made. Sales tax quarters are June-August, September-November, December-February and March-May.

If a person has not closed its books for the sales tax quarter immediately preceding the sales tax quarter in which the certification is being made, such person should use its sales information from the four most recent sales tax quarters for which such information is available to determine whether the more than \$300,000 cumulative sales threshold has been met.

Application of the above rule is illustrated by the following example:

Example: Contractor A is awarded a \$150,000 contract by covered agency B in June, 2006. Contractor A would determine whether the more than \$300,000 threshold was met by examining its sales of tangible personal property or taxable services within New York State during the June, 2005-August, 2005; September, 2005-November, 2005, December, 2005-February, 2006 and March, 2006-May, 2006 sales tax quarters. If Contractor A has not completed its accounting for the March, 2006-May, 2006 sales tax quarter, then it should, in lieu of that sales tax quarter, use data from the March, 2005-May, 2005 sales tax quarter.

19) Q: How are the terms *sale*, *tangible personal property* and *taxable services* defined for purposes of determining whether the more than \$300,000 cumulative sales threshold has been met?

A: *Sale* has the meaning given for New York State and local sales and compensating use tax law purposes, and includes any transfer of title or possession or both, exchange or barter, rental, lease or license to use or consume (including, with respect to computer software, the right to reproduce), conditional or otherwise, in any manner or by any means whatsoever for a consideration, or any agreement therefor.

Tangible personal property has the meaning given for New York State and local sales and compensating use tax purposes. For such purposes, the term means corporeal personal property of any nature having a material existence and perceptible to the human senses. Tangible personal property includes, but is not limited to:

- raw materials, such as wood, metal, rubber and minerals;
- manufactured items, such as gasoline, oil, diesel motor fuel and kero-jet fuel, chemicals, jewelry, furniture, machinery and equipment, parts, tools, supplies, clothing, motor vehicles, appliances, boats, yachts, lighting fixtures, building materials;
- computers and pre-written (canned/off-the-shelf/standard) software;
- artistic items, such as sketches, paintings, photographs, moving picture films and recordings;
- animals, trees, shrubs, plants and seeds;
- bottled water, soda, beer;
- candy and confections;
- cigarettes and tobacco products;
- cosmetics and toiletries;
- coins and other numismatic items, when purchased for purposes other than for use as a medium of exchange;
- postage stamps, when purchased for purposes other than mailing; and
- precious metals in the form of bullion, ingots, wafers and other forms.

Tangible personal property does **not** include real property or intangible personal property.

Taxable services means services, the receipts from the sale of which are taxable for New York State and local sales and compensating use tax purposes. The term includes those services specifically enumerated in New York State and local sales and compensating use tax law as taxable. Taxable services are determined without regard to exemptions provided for in the sales and compensating use tax law. The term includes, but is not limited to:

- providing information by printed, mimeographed or multigraphed matter or by duplicating written or printed matter in any other manner, including the services of collecting, compiling or analyzing information of any kind or nature and furnishing reports thereof to other persons;
- processing, assembling, fabricating, printing or imprinting tangible personal property furnished by a customer who did not purchase the tangible personal property for resale;
- installing tangible personal property, or maintaining, servicing or repairing tangible personal property that is not held for sale by the purchaser of the service;
- storing tangible personal property that is not being held for sale, and the rental of safe deposit boxes or similar space;
- maintaining, servicing or repairing real property, whether inside or outside buildings;
- providing parking, garaging or storing for motor vehicles;
- interior decorating and designing services;
- protective and detective services; and
- furnishing entertainment or information services by means of telephony or telegraphy.

20) Q: Are exempt sales taken into account in determining whether the more than \$300,000 sales threshold of section 5-a is met?

A: Yes. In determining whether more than \$300,000 in sales of tangible personal property or taxable services were made during the specified period, contractors must count exempt sales of tangible personal property or taxable services. Contractors should determine whether sales are of tangible personal property or taxable services with reference to Articles 28 and 29 of the New York State Tax Law, disregarding relevant exemptions provided for therein, including, but not limited to, the exemption for sales to exempt organizations.

Example:

During the four specified sales tax quarterly periods, an out-of-state contractor made \$400,000 in sales of tangible personal property into New York State. The entire \$400,000 in sales during such periods was made to exempt state agencies. The contractor has exceeded the \$300,000 threshold and must be certified as registered for New York State and local sales and compensating use tax purposes.

21) Q: Who is responsible for making the certifications required by section 5-a?

A: The contractor is responsible for making the certifications required by the statute. The contractor's certification must include whether its affiliates and/or subcontractors whose sales exceeded the \$300,000 threshold during the specified period, are registered for New York State sales and compensating use tax purposes. The contractor's certification must be made to the best of its knowledge.

22) Q: How does a contractor make the certifications required by the statute?

A: The contractor must file a properly completed Form ST-220-CA (with the procuring covered agency) and Form ST-220-TD (with the Tax Department). The covered agency must include Form ST-220-CA in the procurement record for the contract.

These requirements must be met before a contract may take effect.

Renewals: In addition, after a contract has taken effect, a Form ST-220-CA must be filed again with a covered agency if a contract, which by its terms may be renewed, is being renewed. In this case, the Form ST-220-CA must be filed with the contracting covered agency prior to the commencement date of the renewal term(s). In addition, a new Form ST-220-TD may be required to be filed with the Tax Department. A new Form ST-220-TD would be required to be filed with the Tax Department if no previous Form ST-220-TD has been filed by the contractor with the Tax Department or, if a previously filed Form ST-220-TD is no longer correct and complete.

Example:

Contractor A is awarded a contract by Covered Agency B. The contract is Contractor A's first with a covered agency, and is subject to the requirements of section 5-a. Contractor A has one affiliate and one subcontractor, and all three entities exceeded the \$300,000 threshold during the specified period. Contractor A must file Form ST-220-TD with the Tax Department, certifying that all three entities are registered for New York State and local sales and compensating use tax purposes. In addition, Contractor A must file Form ST-220-CA with Covered Agency B, certifying that it has filed Form ST-220-TD with the Tax Department, and that it is correct and complete.

During the term of its contract with Covered Agency B, Contractor A acquires two new affiliates and one additional subcontractor. One of the affiliates, as well as the subcontractor, exceeded the \$300,000 threshold during the specified sales tax quarters. Contractor A must, as soon as possible after learning of the changed circumstances, file a new Form ST-220-TD with the Tax Department, certifying that the affiliate and the subcontractor exceeding the \$300,000 threshold are registered for New York State and local sales and compensating use tax purposes. If Contractor A does not file the new Form ST-220-TD with the Tax Department, then the consequences specified in Q&A 31 below could apply.

Contractor A's contract with Covered Agency B provides that the contract may be renewed for one additional two-year term, at the option of the parties. The parties agree to renew the contract. Thus, Contractor A must, prior to the commencement date of the renewal term, file a new Form ST-220-CA with Covered Agency B certifying that it has filed Form ST-220-TD with the Tax Department, and that it is correct and complete. If Contractor A cannot make such certification to Covered Agency B because information shown on the current Form ST-220-TD filed with the Tax Department is not correct and complete, then it must immediately file a new Form ST-220-TD with the Tax Department reflecting current information. Contractor A must then file Form ST-220-CA with Covered Agency B before the commencement date of the renewal term.

Following commencement of Contractor A's renewal term with Covered Agency B, Contractor A is awarded a new contract by Covered Agency C. The new contract is covered by section 5-a. If the information shown on Contractor A's last filed

Form ST-220-TD is correct and complete, it need not file a new Form ST-220-TD with the Tax Department. However, Contractor A must file Form ST-220-CA with Covered Agency C certifying that it has previously filed Form ST-220-TD with the Tax Department, and that it is correct and complete as of the date of the new certification (Form ST-220-CA) filing with Covered Agency C.

- 23) Q:** If the contractor filed Form ST-220 prior to amendment of section 5-a on April 26, 2006, and the contract has, since April 26, 2006, been amended, extended, renewed or assigned, must a Form ST-220-TD be filed with the Tax Department?
- A:** Yes, if the contract meets the criteria set forth in Q & A 3.
- 24) Q:** Must Form ST-220-TD be filed with the Tax Department if the contractor filed Form ST-220 prior to amendment of section 5-a on April 26, 2006, and the contractor is then awarded another contract after that date?
- A:** Yes, if the contract meets the criteria set forth in Q & A 3.
- 25) Q:** When is a contractor, affiliate or subcontractor required to be listed in Schedule A of Form ST-220-TD?
- A:** A contractor, affiliate or subcontractor is required to be listed in Schedule A of Form ST-220-TD when such contractor, affiliate or subcontractor has exceeded the more than \$300,000 cumulative sales threshold during the specified period as discussed in Q & A 18.
- 26) Q:** When is a contractor who previously filed Form ST-220-TD with the Tax Department required to file a new Form ST-220-TD certification with the Tax Department?
- A:** If a contractor or an affiliate or subcontractor, is not registered with the Tax Department for sales and compensating use tax purposes on the contractor's original certification, and such contractor, affiliate, or subcontractor makes sales delivered by any means to locations within New York State of tangible personal property or taxable services having a value in excess of \$300,000 during any consecutive four sales tax quarters which follow the sales tax quarter in which the contractor's original certification was made, then the contractor shall, as soon as possible after such occurrence, file a new Form ST-220-TD with the Tax Department certifying that it, and/or its affiliates and/or subcontractors, as applicable, are registered for sales and compensating use tax purposes.
- 27) Q:** If a contractor, affiliate or subcontractor is required by section 5-a to be registered with the Tax Department to collect New York State and local sales and compensating use taxes, and such person is not registered, what must such person do to register?
- A:** The contractor, affiliate or subcontractor must complete Form DTF-17, *Application to Register for a Sales Tax Certificate of Authority* to register. Upon registration, the Tax Department will issue a certificate of authority, which authorizes the recipient to collect New York State and local sales and compensating use taxes. Form DTF-17 is available on the Tax Department's Web site, www.nystax.gov, or may be obtained by calling the Sales Tax Information Center at 518-485-2889 (in-state callers without free long distance call 1-800-698-2909). For additional information regarding registration, see Publication 750, *A Guide to Sales Tax in New York State*.
- 28) Q:** If a contractor, affiliate or subcontractor has submitted Form DTF-17, to register to collect New York State sales and compensating use taxes at the time of filing the certifications required under section 5-a, but has not yet received its certificate of authority from the Tax Department, how should the contractor complete the certifications?
- A:** The contractor should complete the certifications as required. The column on Schedule A asking whether the person listed is in the process of registering should be checked. If there is a problem with the registration (see Tax Law section 1134(a)(4)(B) for reasons why registration may be denied), the Tax Department will notify the applicant.
- 29) Q:** Who is responsible for signing Forms ST-220-TD and ST-220-CA?
- A:** An individual authorized to sign on behalf of the contractor may execute the certifications.
- 30) Q:** Can Form ST-220-TD be provided to the Tax Department electronically?
- A:** Form ST-220-TD **cannot** be provided electronically to the Tax Department at this time. If the Tax Department later determines that electronic submission is feasible, instructions will be issued as to how to electronically sign and file Form ST-220-TD.

- 31) Q:** What are the consequences if Form ST-220-TD and/or Form ST-220-CA are not provided, or if provided, are determined to be false?
- A:** If a contractor fails to make the certifications required by section 5-a, by law, the contract cannot take effect. If during the term of the contract, the Tax Department or the covered agency discovers that a certification is false, then such false certification may subject the contractor to civil or criminal sanctions, and a finding of nonresponsibility for future procurements. Under certain circumstances, the statute provides that the contract shall be subject to termination if the covered agency determines that termination of the contract is in the best interests of New York State.
- 32) Q:** What is the effect of registering with the Tax Department to collect New York State and local sales and compensating use taxes?
- A:** Once registered, a person is a *vendor* within the meaning of New York State and local sales and compensating use tax law, and must file returns and collect and pay, or pay over, tax. Failure to file returns and collect and pay, or pay over, tax will result in imposition of penalty and interest charges.

Need help?



Visit our Web site at **www.tax.ny.gov**

- get information and manage your taxes online
- check for new online services and features



Telephone assistance

Sales Tax Information Center: (518) 485-2889

To order forms and publications: (518) 457-5431



Text Telephone (TTY) Hotline (for persons with hearing and speech disabilities using a TTY): If you have access to a TTY, contact us at (518) 485-5082. If you do not own a TTY, check with independent living centers or community action programs to find out where machines are available for public use.



Persons with disabilities: In compliance with the Americans with Disabilities Act, we will ensure that our lobbies, offices, meeting rooms, and other facilities are accessible to persons with disabilities. If you have questions about special accommodations for persons with disabilities, call the information center.

This Page Intentionally Blank

**Contractor Certification to Covered Agency**

(Pursuant to Section 5-a of the Tax Law, as amended, effective April 26, 2006)

ST-220-CA

(12/11)

For information, consult Publication 223, Questions and Answers Concerning Tax Law Section 5-a (see Need Help? on back).

Contractor name				For covered agency use only Contract number or description		
Contractor's principal place of business		City	State			ZIP code
Contractor's mailing address (if different than above)						Estimated contract value over the full term of contract (but not including renewals)
Contractor's federal employer identification number (EIN)			Contractor's sales tax ID number (if different from contractor's EIN)			
Contractor's telephone number		Covered agency name				\$
Covered agency address					Covered agency telephone number	

I, _____, hereby affirm, under penalty of perjury, that I am _____
(name) (title)

of the above-named contractor, that I am authorized to make this certification on behalf of such contractor, and I further certify that:

(Mark an X in only one box)

☐ The contractor has filed Form ST-220-TD with the Department of Taxation and Finance in connection with this contract and, to the best of contractor's knowledge, the information provided on the Form ST-220-TD, is correct and complete.

☐ The contractor has previously filed Form ST-220-TD with the Tax Department in connection with _____
(insert contract number or description)

and, to the best of the contractor's knowledge, the information provided on that previously filed Form ST-220-TD, is correct and complete as of the current date, and thus the contractor is not required to file a new Form ST-220-TD at this time.

Sworn to this ____ day of _____, 20 ____

(sign before a notary public)

(title)

Instructions

General information

Tax Law section 5-a was amended, effective April 26, 2006. On or after that date, in all cases where a contract is subject to Tax Law section 5-a, a contractor must file (1) Form ST-220-CA, *Contractor Certification to Covered Agency*, with a covered agency, and (2) Form ST-220-TD with the Tax Department before a contract may take effect. The circumstances when a contract is subject to section 5-a are listed in Publication 223, Q&A 3. See *Need help?* for more information on how to obtain this publication. In addition, a contractor must file a new Form ST-220-CA with a covered agency before an existing contract with such agency may be renewed.

Note: Form ST-220-CA must be signed by a person authorized to make the certification on behalf of the contractor, and the acknowledgement on page 2 of this form must be completed before a notary public.

When to complete this form

As set forth in Publication 223, a contract is subject to section 5-a, and you must make the required certification(s), if:

- The procuring entity is a *covered agency* within the meaning of the statute (see Publication 223, Q&A 5);
- The contractor is a *contractor* within the meaning of the statute (see Publication 223, Q&A 6); and
- The contract is a *contract* within the meaning of the statute. This is the case when it (a) has a value in excess of \$100,000 and (b) is a contract for *commodities* or *services*, as such terms are defined for purposes of the statute (see Publication 223, Q&A 8 and 9).

Furthermore, the procuring entity must have begun the solicitation to purchase on or after January 1, 2005, and the resulting contract must have been awarded, amended, extended, renewed, or assigned *on or after April 26, 2006* (the effective date of the section 5-a amendments).

Individual, Corporation, Partnership, or LLC Acknowledgment

STATE OF _____ }
: _____ SS.:
COUNTY OF _____ }

On the ____ day of _____ in the year 20____, before me personally appeared _____, known to me to be the person who executed the foregoing instrument, who, being duly sworn by me did depose and say that _____ he resides at _____, Town of _____, County of _____, State of _____; and further that:

[Mark an **X** in the appropriate box and complete the accompanying statement.]

- ☐ (If an individual): _____ he executed the foregoing instrument in his/her name and on his/her own behalf.
- ☐ (If a corporation): _____ he is the _____ of _____, the corporation described in said instrument; that, by authority of the Board of Directors of said corporation, _____ he is authorized to execute the foregoing instrument on behalf of the corporation for purposes set forth therein; and that, pursuant to that authority, _____ he executed the foregoing instrument in the name of and on behalf of said corporation as the act and deed of said corporation.
- ☐ (If a partnership): _____ he is a _____ of _____, the partnership described in said instrument; that, by the terms of said partnership, _____ he is authorized to execute the foregoing instrument on behalf of the partnership for purposes set forth therein; and that, pursuant to that authority, _____ he executed the foregoing instrument in the name of and on behalf of said partnership as the act and deed of said partnership.
- ☐ (If a limited liability company): _____ he is a duly authorized member of _____, LLC, the limited liability company described in said instrument; that _____ he is authorized to execute the foregoing instrument on behalf of the limited liability company for purposes set forth therein; and that, pursuant to that authority, _____ he executed the foregoing instrument in the name of and on behalf of said limited liability company as the act and deed of said limited liability company.

Notary Public

Registration No.

Privacy notification

The Commissioner of Taxation and Finance may collect and maintain personal information pursuant to the New York State Tax Law, including but not limited to, sections 5-a, 171, 171-a, 287, 308, 429, 475, 505, 697, 1096, 1142, and 1415 of that Law; and may require disclosure of social security numbers pursuant to 42 USC 405(c)(2)(C)(i).

This information will be used to determine and administer tax liabilities and, when authorized by law, for certain tax offset and exchange of tax information programs as well as for any other lawful purpose.

Information concerning quarterly wages paid to employees is provided to certain state agencies for purposes of fraud prevention, support enforcement, evaluation of the effectiveness of certain employment and training programs and other purposes authorized by law.

Failure to provide the required information may subject you to civil or criminal penalties, or both, under the Tax Law.

This information is maintained by the Manager of Document Management, NYS Tax Department, W A Harriman Campus, Albany NY 12227; telephone (518) 457-5181.

Need help?



Visit our Web site at **www.tax.ny.gov**

- get information and manage your taxes online
- check for new online services and features



Telephone assistance

Sales Tax Information Center: (518) 485-2889

To order forms and publications: (518) 457-5431

Text Telephone (TTY) Hotline (for persons with hearing and speech disabilities using a TTY): (518) 485-5082



Persons with disabilities: In compliance with the Americans with Disabilities Act, we will ensure that our lobbies, offices, meeting rooms, and other facilities are accessible to persons with disabilities. If you have questions about special accommodations for persons with disabilities, call the information center.

**Contractor Certification**(Pursuant to Section 5-a of the Tax Law, as amended,
effective April 26, 2006)**ST-220-TD**

(12/11)

For information, consult Publication 223, *Questions and Answers Concerning Tax Law Section 5-a* (see *Need help?* below).

Contractor name

Contractor's principal place of business

City

State

ZIP code

Contractor's mailing address (if different than above)

Contractor's federal employer identification number (EIN)

Contractor's sales tax ID number (if different from contractor's EIN)

Contractor's telephone number
()

Covered agency or state agency

Contract number or description

Estimated contract value over
the full term of contract
(but not including renewals) \$

Covered agency address

Covered agency telephone number

General information

Section 5-a of the Tax Law, as amended, effective April 26, 2006, requires certain contractors awarded certain state contracts valued at more than \$100,000 to certify to the Tax Department that they are registered to collect New York State and local sales and compensating use taxes, if they made sales delivered by any means to locations within New York State of tangible personal property or taxable services having a cumulative value in excess of \$300,000, measured over a specified period. In addition, contractors must certify to the Tax Department that each affiliate and subcontractor exceeding such sales threshold during a specified period is registered to collect New York State and local sales and compensating use taxes. Contractors must also file a Form ST-220-CA, certifying to the procuring state entity that they filed Form ST-220-TD with the Tax Department and that the information contained on Form ST-220-TD is correct and complete as of the date they file Form ST-220-CA.

All sections must be completed including all fields on the top of this page, all sections on page 2, Schedule A on page 3, if applicable, and Individual, Corporation, Partnership, or LLC Acknowledgement on page 4. If you do not complete these areas, the form will be returned to you for completion.

For more detailed information regarding this form and section 5-a of the Tax Law, see Publication 223, *Questions and Answers Concerning Tax Law Section 5-a, (as amended, effective April 26, 2006)*. See *Need help?* for more information on how to obtain this publication.

Note: Form ST-220-TD must be signed by a person authorized to make the certification on behalf of the contractor, and the acknowledgement on page 4 of this form must be completed before a notary public.

Mail completed form to:

**NYS TAX DEPARTMENT
DATA ENTRY SECTION
W A HARRIMAN CAMPUS
ALBANY NY 12227****Privacy notification**

The Commissioner of Taxation and Finance may collect and maintain personal information pursuant to the New York State Tax Law, including but not limited to, sections 5-a, 171, 171-a, 287, 308, 429, 475, 505, 697, 1096, 1142, and 1415 of that Law; and may require disclosure of social security numbers pursuant to 42 USC 405(c)(2)(C)(i).

This information will be used to determine and administer tax liabilities and, when authorized by law, for certain tax offset and exchange of tax information programs as well as for any other lawful purpose.

Information concerning quarterly wages paid to employees is provided to certain state agencies for purposes of fraud prevention, support enforcement, evaluation of the effectiveness of certain employment and training programs and other purposes authorized by law.

Failure to provide the required information may subject you to civil or criminal penalties, or both, under the Tax Law.

This information is maintained by the Manager of Document Management, NYS Tax Department, W A Harriman Campus, Albany NY 12227; telephone (518) 457-5181.

Need help?Visit our Web site at **www.tax.ny.gov**

- get information and manage your taxes online
- check for new online services and features

**Telephone assistance****Sales Tax** Information Center: (518) 485-2889

To order forms and publications: (518) 457-5431

Text Telephone (TTY) Hotline (for persons with hearing and speech disabilities using a TTY): (518) 485-5082

Persons with disabilities: In compliance with the Americans with Disabilities Act, we will ensure that our lobbies, offices, meeting rooms, and other facilities are accessible to persons with disabilities. If you have questions about special accommodations for persons with disabilities, call the information center.

I, _____, hereby affirm, under penalty of perjury, that I am _____
(name) (title)
of the above-named contractor, and that I am authorized to make this certification on behalf of such contractor.

Complete Sections 1, 2, and 3 below. Make only one entry in each section.

Section 1 — Contractor registration status

- ☐ The contractor has made sales delivered by any means to locations within New York State of tangible personal property or taxable services having a cumulative value in excess of \$300,000 during the four sales tax quarters which immediately precede the sales tax quarter in which this certification is made. The contractor is registered to collect New York State and local sales and compensating use taxes with the Commissioner of Taxation and Finance pursuant to sections 1134 and 1253 of the Tax Law, and is listed on Schedule A of this certification.
- ☐ The contractor has not made sales delivered by any means to locations within New York State of tangible personal property or taxable services having a cumulative value in excess of \$300,000 during the four sales tax quarters which immediately precede the sales tax quarter in which this certification is made.

Section 2 — Affiliate registration status

- ☐ The contractor does not have any affiliates.
- ☐ To the best of the contractor's knowledge, the contractor has one or more affiliates having made sales delivered by any means to locations within New York State of tangible personal property or taxable services having a cumulative value in excess of \$300,000 during the four sales tax quarters which immediately precede the sales tax quarter in which this certification is made, and each affiliate exceeding the \$300,000 cumulative sales threshold during such quarters is registered to collect New York State and local sales and compensating use taxes with the Commissioner of Taxation and Finance pursuant to sections 1134 and 1253 of the Tax Law. The contractor has listed each affiliate exceeding the \$300,000 cumulative sales threshold during such quarters on Schedule A of this certification.
- ☐ To the best of the contractor's knowledge, the contractor has one or more affiliates, and each affiliate has not made sales delivered by any means to locations within New York State of tangible personal property or taxable services having a cumulative value in excess of \$300,000 during the four sales tax quarters which immediately precede the sales tax quarter in which this certification is made.

Section 3 — Subcontractor registration status

- ☐ The contractor does not have any subcontractors.
- ☐ To the best of the contractor's knowledge, the contractor has one or more subcontractors having made sales delivered by any means to locations within New York State of tangible personal property or taxable services having a cumulative value in excess of \$300,000 during the four sales tax quarters which immediately precede the sales tax quarter in which this certification is made, and each subcontractor exceeding the \$300,000 cumulative sales threshold during such quarters is registered to collect New York State and local sales and compensating use taxes with the Commissioner of Taxation and Finance pursuant to sections 1134 and 1253 of the Tax Law. The contractor has listed each subcontractor exceeding the \$300,000 cumulative sales threshold during such quarters on Schedule A of this certification.
- ☐ To the best of the contractor's knowledge, the contractor has one or more subcontractors, and each subcontractor has not made sales delivered by any means to locations within New York State of tangible personal property or taxable services having a cumulative value in excess of \$300,000 during the four sales tax quarters which immediately precede the sales tax quarter in which this certification is made.

Sworn to this ____ day of _____, 20 ____

(sign before a notary public)

(title)

Schedule A — Listing of each entity (contractor, affiliate, or subcontractor) exceeding \$300,000 cumulative sales threshold

List the contractor, or affiliate, or subcontractor in Schedule A only if such entity exceeded the \$300,000 cumulative sales threshold during the specified sales tax quarters. See directions below. For more information, see Publication 223.

[illegible]

Column A – Enter **C** in column A if the contractor; **A** if an affiliate of the contractor; or **S** if a subcontractor.

Column B – Name - If the entity is a corporation or limited liability company, enter the exact legal name as registered with the NY Department of State, if applicable. If the entity is a partnership or sole proprietor, enter the name of the partnership and each partner's given name, or the given name(s) of the owner(s), as applicable. If the entity has a different DBA (doing business as) name, enter that name as well.

Column C – Address - Enter the street address of the entity's principal place of business. Do not enter a PO box.

Column D – ID number - Enter the federal employer identification number (EIN) assigned to the entity. If the entity is an individual, enter the social security number of that person.

Column E – Sales tax ID number - Enter only if different from federal EIN in column D.

Column F – If applicable, enter an X if the entity has submitted Form DTF-17 to the Tax Department but has not received its certificate of authority as of the date of this certification.

Individual, Corporation, Partnership, or LLC Acknowledgment

STATE OF }
 : SS.:
COUNTY OF }

On the ____ day of _____ in the year 20____, before me personally appeared _____, known to me to be the person who executed the foregoing instrument, who, being duly sworn by me did depose and say that
_ he resides at _____,
Town of _____,
County of _____,
State of _____; and further that:

[Mark an **X** in the appropriate box and complete the accompanying statement.]

☐ (If an individual): _he executed the foregoing instrument in his/her name and on his/her own behalf.

☐ (If a corporation): _he is the _____
of _____, the corporation described in said instrument; that, by authority of the Board of Directors of said corporation, _he is authorized to execute the foregoing instrument on behalf of the corporation for purposes set forth therein; and that, pursuant to that authority, _he executed the foregoing instrument in the name of and on behalf of said corporation as the act and deed of said corporation.

☐ (If a partnership): _he is a _____
of _____, the partnership described in said instrument; that, by the terms of said partnership, _he is authorized to execute the foregoing instrument on behalf of the partnership for purposes set forth therein; and that, pursuant to that authority, _he executed the foregoing instrument in the name of and on behalf of said partnership as the act and deed of said partnership.

☐ (If a limited liability company): _he is a duly authorized member of _____
LLC, the limited liability company described in said instrument; that _he is authorized to execute the foregoing instrument on behalf of the limited liability company for purposes set forth therein; and that, pursuant to that authority, _he executed the foregoing instrument in the name of and on behalf of said limited liability company as the act and deed of said limited liability company.

Notary Public

Registration No. _____

Attachment 16

Vendor Responsibility Questionnaire

Intentionally Blank

NEW YORK STATE VENDOR RESPONSIBILITY QUESTIONNAIRE FOR-PROFIT BUSINESS ENTITY

You have selected the For-Profit Non-Construction questionnaire which may be printed and completed in this format or, for your convenience, may be completed online using the New York State VendRep System.

COMPLETION & CERTIFICATION

The person(s) completing the questionnaire must be knowledgeable about the vendor's business and operations. An owner or officer must certify the questionnaire and the signature must be notarized.

NEW YORK STATE VENDOR IDENTIFICATION NUMBER (VENDOR ID)

The Vendor ID is a ten-digit identifier issued by New York State when the vendor is registered on the Statewide Vendor File. This number must now be included on the questionnaire. If the business entity has not obtained a Vendor ID, contact the OSC Help Desk at ciohelpdesk@osc.state.ny.us or call 866-370-4672.

DEFINITIONS

All underlined terms are defined in the "New York State Vendor Responsibility Definitions List," found at www.osc.state.ny.us/vendrep/documents/questionnaire/definitions.pdf. These terms may not have their ordinary, common or traditional meanings. Each vendor is strongly encouraged to read the respective definitions for any and all underlined terms. By submitting this questionnaire, the vendor agrees to be bound by the terms as defined in the "New York State Vendor Responsibility Definitions List" existing at the time of certification.

RESPONSES

Every question must be answered. Each response must provide all relevant information which can be obtained within the limits of the law. However, information regarding a determination or finding made in error which was subsequently corrected is not required. Individuals and Sole Proprietors may use a Social Security Number but are encouraged to obtain and use a federal Employer Identification Number (EIN).

REPORTING ENTITY

Each vendor must indicate if the questionnaire is filed on behalf of the entire Legal Business Entity or an Organizational Unit within or operating under the authority of the Legal Business Entity and having the same EIN. Generally, the Organizational Unit option may be appropriate for a vendor that meets the definition of "Reporting Entity" but due to the size and complexity of the Legal Business Entity, is best able to provide the required information for the Organizational Unit, while providing more limited information for other parts of the Legal Business Entity and Associated Entities.

ASSOCIATED ENTITY

An Associated Entity is one that owns or controls the Reporting Entity or any entity owned or controlled by the Reporting Entity. However, the term Associated Entity does **not** include "sibling organizations" (i.e., entities owned or controlled by a parent company that owns or controls the Reporting Entity), unless such sibling entity has a direct relationship with or impact on the Reporting Entity.

STRUCTURE OF THE QUESTIONNAIRE

The questionnaire is organized into eleven sections. Section I is to be completed for the Legal Business Entity. Section II requires the vendor to specify the Reporting Entity for the questionnaire. Section III refers to the individuals of the Reporting Entity, while Sections IV-VIII require information about the Reporting Entity. Section IX pertains to any Associated Entities, with one question about their Officials/Owners. Section X relates to disclosure under the Freedom of Information Law (FOIL). Section XI requires an authorized contact for the questionnaire information.

**NEW YORK STATE
VENDOR RESPONSIBILITY QUESTIONNAIRE
FOR-PROFIT BUSINESS ENTITY**

I. LEGAL BUSINESS ENTITY INFORMATION			
<u>Legal Business Entity Name*</u>		<u>EIN</u>	
Address of the <u>Principal Place of Business</u> (street, city, state, zip code)		<u>New York State Vendor Identification Number</u>	
		Telephone ext.	Fax
Email		Website	
Additional <u>Legal Business Entity</u> Identities: If applicable, list any other <u>DBA</u> , <u>Trade Name</u> , <u>Former Name</u> , Other Identity, or <u>EIN</u> used in the last five (5) years and the status (active or inactive).			
Type	Name	EIN	Status
1.0 <u>Legal Business Entity</u> Type – Check appropriate box and provide additional information:			
☐ <u>Corporation</u> (including <u>PC</u>)		Date of Incorporation	
☐ <u>Limited Liability Company (LLC or PLLC)</u>		Date of Organization	
☐ <u>Partnership</u> (including <u>LLP</u> , <u>LP</u> or <u>General</u>)		Date of Registration or Establishment	
☐ <u>Sole Proprietor</u>		How many years in business?	
☐ Other		Date Established	
If Other, explain:			
1.1 Was the <u>Legal Business Entity</u> formed or incorporated in New York State?			☐ Yes ☐ No
If ‘No,’ indicate jurisdiction where <u>Legal Business Entity</u> was formed or incorporated and attach a <u>Certificate of Good Standing</u> from the applicable jurisdiction or provide an explanation if a <u>Certificate of Good Standing</u> is not available.			
☐ United States State _____			
☐ Other Country _____			
Explain, if not available:			
1.2 Is the <u>Legal Business Entity</u> publicly traded?			☐ Yes ☐ No
If “Yes,” provide <u>CIK Code</u> or Ticker Symbol			
1.3 Does the <u>Legal Business Entity</u> have a <u>DUNS</u> Number?			☐ Yes ☐ No
If “Yes,” Enter <u>DUNS</u> Number			

* All underlined terms are defined in the “New York State Vendor Responsibility Definitions List,” which can be found at www.osc.state.ny.us/vendrep/documents/questionnaire/definitions.pdf.

**NEW YORK STATE
VENDOR RESPONSIBILITY QUESTIONNAIRE
FOR-PROFIT BUSINESS ENTITY**

I. LEGAL BUSINESS ENTITY INFORMATION

- 1.4 If the Legal Business Entity's Principal Place of Business is not in New York State, does the Legal Business Entity maintain an office in New York State?
(Select "N/A," if Principal Place of Business is in New York State.)
- ☐ Yes ☐ No
☐ N/A

If "Yes," provide the address and telephone number for one office located in New York State.

- 1.5 Is the Legal Business Entity a New York State certified Minority-Owned Business Enterprise (MBE), Women-Owned Business Enterprise (WBE), New York State Small Business (SB) or a federally certified Disadvantaged Business Enterprise (DBE)?
- If "Yes," check all that apply:
- ☐ New York State certified Minority-Owned Business Enterprise (MBE)
☐ New York State certified Women-Owned Business Enterprise (WBE)
☐ New York State Small Business (SB)
☐ Federally certified Disadvantaged Business Enterprise (DBE)
- ☐ Yes ☐ No

- 1.6 Identify Officials and Principal Owners, if applicable. For each person, include name, title and percentage of ownership. Attach additional pages if necessary. If applicable, reference to relevant SEC filing(s) containing the required information is optional.

Name	Title	Percentage Ownership (Enter 0% if not applicable)

**NEW YORK STATE
VENDOR RESPONSIBILITY QUESTIONNAIRE
FOR-PROFIT BUSINESS ENTITY**

II. REPORTING ENTITY INFORMATION

2.0 The Reporting Entity for this questionnaire is:

Note: Select only one.

☐ Legal Business Entity

Note: If selecting this option, “Reporting Entity” refers to the entire Legal Business Entity for the remainder of the questionnaire. (SKIP THE REMAINDER OF SECTION II AND PROCEED WITH SECTION III.)

☐ Organizational Unit within and operating under the authority of the Legal Business Entity

SEE DEFINITIONS OF “REPORTING ENTITY” AND “ORGANIZATIONAL UNIT” FOR ADDITIONAL INFORMATION ON CRITERIA TO QUALIFY FOR THIS SELECTION.

Note: If selecting this option, “Reporting Entity” refers to the Organizational Unit within the Legal Business Entity for the remainder of the questionnaire. (COMPLETE THE REMAINDER OF SECTION II AND ALL REMAINING SECTIONS OF THIS QUESTIONNAIRE.)

IDENTIFYING INFORMATION

a) Reporting Entity Name

Address of the Primary Place of Business (street, city, state, zip code)

Telephone

ext.

b) Describe the relationship of the Reporting Entity to the Legal Business Entity

c) Attach an organizational chart

d) Does the Reporting Entity have a DUNS Number?

☐ Yes ☐ No

If “Yes,” enter DUNS Number

e) Identify the designated manager(s) responsible for the business of the Reporting Entity.

For each person, include name and title. Attach additional pages if necessary.

Name

Title

**NEW YORK STATE
VENDOR RESPONSIBILITY QUESTIONNAIRE
FOR-PROFIT BUSINESS ENTITY**

INSTRUCTIONS FOR SECTIONS III THROUGH VII

For each “Yes,” provide an explanation of the issue(s), relevant dates, the government entity involved, any remedial or corrective action(s) taken and the current status of the issue(s). For each “Other,” provide an explanation which provides the basis for not definitively responding “Yes” or “No.” Provide the explanation at the end of the section or attach additional sheets with numbered responses, including the Reporting Entity name at the top of any attached pages.

III. LEADERSHIP INTEGRITY

Within the past five (5) years, has any current or former reporting entity official or any individual currently or formerly having the authority to sign, execute or approve bids, proposals, contracts or supporting documentation on behalf of the reporting entity with any government entity been:

3.0 <u>Sanctioned</u> relative to any business or professional permit and/or license?	☐ Yes ☐ No ☐ Other
3.1 <u>Suspended, debarred, or disqualified</u> from any <u>government contracting process</u> ?	☐ Yes ☐ No ☐ Other
3.2 The subject of an <u>investigation</u> , whether open or closed, by any <u>government entity</u> for a civil or criminal violation for any business-related conduct?	☐ Yes ☐ No ☐ Other
3.3 Charged with a misdemeanor or felony, indicted, granted immunity, convicted of a crime or subject to a <u>judgment</u> for: a) Any business-related activity; or b) Any crime, whether or not business-related, the underlying conduct of which was related to truthfulness?	☐ Yes ☐ No ☐ Other

For each “Yes” or “Other” explain:

IV. INTEGRITY – CONTRACT BIDDING

Within the past five (5) years, has the reporting entity:

4.0 Been <u>suspended</u> or <u>debarred</u> from any <u>government contracting process</u> or been <u>disqualified</u> on any government procurement, permit, license, concession, franchise or lease, including, but not limited to, <u>debarment</u> for a violation of New York State Workers’ Compensation or Prevailing Wage laws or New York State Procurement Lobbying Law?	☐ Yes ☐ No
4.1 Been subject to a denial or revocation of a government prequalification?	☐ Yes ☐ No
4.2 Been denied a contract award or had a bid rejected based upon a <u>non-responsibility finding</u> by a <u>government entity</u> ?	☐ Yes ☐ No
4.3 Had a low bid rejected on a <u>government contract</u> for failure to <u>make good faith efforts</u> on any <u>Minority-Owned Business Enterprise</u> , <u>Women-Owned Business Enterprise</u> or <u>Disadvantaged Business Enterprise</u> goal or <u>statutory affirmative action requirements</u> on a previously held contract?	☐ Yes ☐ No
4.4 Agreed to a voluntary exclusion from bidding/contracting with a <u>government entity</u> ?	☐ Yes ☐ No
4.5 Initiated a request to withdraw a bid submitted to a <u>government entity</u> in lieu of responding to an information request or subsequent to a formal request to appear before the <u>government entity</u> ?	☐ Yes ☐ No

For each “Yes,” explain:

**NEW YORK STATE
VENDOR RESPONSIBILITY QUESTIONNAIRE
FOR-PROFIT BUSINESS ENTITY**

V. INTEGRITY – CONTRACT AWARD*Within the past five (5) years, has the reporting entity:*

5.0 Been <u>suspended</u> , cancelled or <u>terminated for cause</u> on any <u>government contract</u> including, but not limited to, a <u>non-responsibility finding</u> ?	☐ Yes ☐ No
5.1 Been subject to an <u>administrative proceeding</u> or civil action seeking specific performance or restitution in connection with any <u>government contract</u> ?	☐ Yes ☐ No
5.2 Entered into a formal monitoring agreement as a condition of a contract award from a <u>government entity</u> ?	☐ Yes ☐ No
For each “Yes,” explain:	

VI. CERTIFICATIONS/LICENSES*Within the past five (5) years, has the reporting entity:*

6.0 Had a revocation, <u>suspension</u> or <u>disbarment</u> of any business or professional permit and/or license?	☐ Yes ☐ No
6.1 Had a denial, decertification, revocation or forfeiture of New York State certification of <u>Minority-Owned Business Enterprise</u> , <u>Women-Owned Business Enterprise</u> or federal certification of <u>Disadvantaged Business Enterprise</u> status for other than a change of ownership?	☐ Yes ☐ No
For each “Yes,” explain:	

VII. LEGAL PROCEEDINGS*Within the past five (5) years, has the reporting entity:*

7.0 Been the subject of an <u>investigation</u> , whether open or closed, by any <u>government entity</u> for a civil or criminal violation?	☐ Yes ☐ No
7.1 Been the subject of an indictment, grant of immunity, <u>judgment</u> or conviction (including entering into a plea bargain) for conduct constituting a crime?	☐ Yes ☐ No
7.2 Received any OSHA citation and Notification of Penalty containing a violation classified as <u>serious</u> or <u>willful</u> ?	☐ Yes ☐ No
7.3 Had a <u>government entity</u> find a willful prevailing wage or supplemental payment violation or any other willful violation of New York State Labor Law?	☐ Yes ☐ No
7.4 Entered into a consent order with the New York State Department of Environmental Conservation, or received an enforcement determination by any <u>government entity</u> involving a violation of federal, state or local environmental laws?	☐ Yes ☐ No
7.5 Other than previously disclosed: a) Been subject to fines or penalties imposed by <u>government entities</u> which in the aggregate total \$25,000 or more; or b) Been convicted of a criminal offense pursuant to any administrative and/or regulatory action taken by any <u>government entity</u> ?	☐ Yes ☐ No
For each “Yes,” explain:	

NEW YORK STATE
VENDOR RESPONSIBILITY QUESTIONNAIRE
FOR-PROFIT BUSINESS ENTITY

VIII. FINANCIAL AND ORGANIZATIONAL CAPACITY

8.0 Within the past five (5) years, has the <u>Reporting Entity</u> received any <u>formal unsatisfactory performance assessment(s)</u> from any <u>government entity</u> on any contract?	☐ Yes ☐ No
If “Yes,” provide an explanation of the issue(s), relevant dates, the <u>government entity</u> involved, any remedial or corrective action(s) taken and the current status of the issue(s). Provide answer below or attach additional sheets with numbered responses.	
8.1 Within the past five (5) years, has the <u>Reporting Entity</u> had any <u>liquidated damages</u> assessed over \$25,000?	☐ Yes ☐ No
If “Yes,” provide an explanation of the issue(s), relevant dates, contracting party involved, the amount assessed and the current status of the issue(s). Provide answer below or attach additional sheets with numbered responses.	
8.2 Within the past five (5) years, have any <u>liens</u> or <u>judgments</u> (not including UCC filings) over \$25,000 been filed against the <u>Reporting Entity</u> which remain undischarged?	☐ Yes ☐ No
If “Yes,” provide an explanation of the issue(s), relevant dates, the Lien holder or Claimant’s name(s), the amount of the <u>lien(s)</u> and the current status of the issue(s). Provide answer below or attach additional sheets with numbered responses.	
8.3 In the last seven (7) years, has the <u>Reporting Entity</u> initiated or been the subject of any bankruptcy proceedings, whether or not closed, or is any bankruptcy proceeding pending?	☐ Yes ☐ No
If “Yes,” provide the bankruptcy chapter number, the court name and the docket number. Indicate the current status of the proceedings as “Initiated,” “Pending” or “Closed.” Provide answer below or attach additional sheets with numbered responses.	
8.4 During the past three (3) years, has the <u>Reporting Entity</u> failed to file or pay any tax returns required by <u>federal</u> , state or local tax laws?	☐ Yes ☐ No
If “Yes,” provide the taxing jurisdiction, the type of tax, the liability year(s), the tax liability amount the <u>Reporting Entity</u> failed to file/pay and the current status of the tax liability. Provide answer below or attach additional sheets with numbered responses.	
8.5 During the past three (3) years, has the <u>Reporting Entity</u> failed to file or pay any New York State unemployment insurance returns?	☐ Yes ☐ No
If “Yes,” provide the years the <u>Reporting Entity</u> failed to file/pay the insurance, explain the situation and any remedial or corrective action(s) taken and the current status of the issue(s). Provide answer below or attach additional sheets with numbered responses.	
8.6 During the past three (3) years, has the <u>Reporting Entity</u> had any <u>government audit(s)</u> completed?	☐ Yes ☐ No
a) If “Yes,” did any audit of the <u>Reporting Entity</u> identify any reported significant deficiencies in internal control, fraud, illegal acts, significant violations of provisions of contract or grant agreements, significant abuse or any <u>material disallowance</u> ?	☐ Yes ☐ No
If “Yes” to 8.6 a), provide an explanation of the issue(s), relevant dates, the <u>government entity</u> involved, any remedial or corrective action(s) taken and the current status of the issue(s). Provide answer below or attach additional sheets with numbered responses.	

**NEW YORK STATE
VENDOR RESPONSIBILITY QUESTIONNAIRE
FOR-PROFIT BUSINESS ENTITY**

IX. ASSOCIATED ENTITIES

*This section pertains to any entity(ies) that either controls or is controlled by the reporting entity.
(See definition of “associated entity” for additional information to complete this section.)*

9.0 Does the Reporting Entity have any Associated Entities?

☐ Yes ☐ No

Note: All questions in this section must be answered if the Reporting Entity is either:

- An Organizational Unit; or
- The entire Legal Business Entity which controls, or is controlled by, any other entity(ies).

If “No,” SKIP THE REMAINDER OF SECTION IX AND PROCEED WITH SECTION X.

9.1 Within the past five (5) years, has any Associated Entity Official or Principal Owner been charged with a misdemeanor or felony, indicted, granted immunity, convicted of a crime or subject to a judgment for:

☐ Yes ☐ No

- a) Any business-related activity; or
- b) Any crime, whether or not business-related, the underlying conduct of which was related to truthfulness?

If “Yes,” provide an explanation of the issue(s), the individual involved, his/her title and role in the Associated Entity, his/her relationship to the Reporting Entity, relevant dates, the government entity involved, any remedial or corrective action(s) taken and the current status of the issue(s).

9.2 Does any Associated Entity have any currently undischarged federal, New York State, New York City or New York local government liens or judgments (not including UCC filings) over \$50,000?

☐ Yes ☐ No

If “Yes,” provide an explanation of the issue(s), identify the Associated Entity’s name(s), EIN(s), primary business activity, relationship to the Reporting Entity, relevant dates, the Lien holder or Claimant’s name(s), the amount of the lien(s) and the current status of the issue(s). Provide answer below or attach additional sheets with numbered responses.

9.3 Within the past five (5) years, has any Associated Entity:

a) Been disqualified, suspended or debarred from any federal, New York State, New York City or other New York local government contracting process?

☐ Yes ☐ No

b) Been denied a contract award or had a bid rejected based upon a non-responsibility finding by any federal, New York State, New York City, or New York local government entity?

☐ Yes ☐ No

c) Been suspended, cancelled or terminated for cause (including for non-responsibility) on any federal, New York State, New York City or New York local government contract?

☐ Yes ☐ No

d) Been the subject of an investigation, whether open or closed, by any federal, New York State, New York City, or New York local government entity for a civil or criminal violation with a penalty in excess of \$500,000?

☐ Yes ☐ No

e) Been the subject of an indictment, grant of immunity, judgment, or conviction (including entering into a plea bargain) for conduct constituting a crime?

☐ Yes ☐ No

f) Been convicted of a criminal offense pursuant to any administrative and/or regulatory action taken by any federal, New York State, New York City, or New York local government entity?

☐ Yes ☐ No

g) Initiated or been the subject of any bankruptcy proceedings, whether or not closed, or is any bankruptcy proceeding pending?

☐ Yes ☐ No

For each “Yes,” provide an explanation of the issue(s), identify the Associated Entity’s name(s), EIN(s), primary business activity, relationship to the Reporting Entity, relevant dates, the government entity involved, any remedial or corrective action(s) taken and the current status of the issue(s). Provide answer below or attach additional sheets with numbered responses.

**NEW YORK STATE
VENDOR RESPONSIBILITY QUESTIONNAIRE
FOR-PROFIT BUSINESS ENTITY**

X. FREEDOM OF INFORMATION LAW (FOIL)

10. Indicate whether any information supplied herein is believed to be exempt from disclosure under the Freedom of Information Law (FOIL).
Note: A determination of whether such information is exempt from FOIL will be made at the time of any request for disclosure under FOIL.

☐ Yes ☐ No

If "Yes," indicate the question number(s) and explain the basis for the claim.

XI. AUTHORIZED CONTACT FOR THIS QUESTIONNAIRE

Name	Telephone ext.	Fax
Title	Email	

**NEW YORK STATE
VENDOR RESPONSIBILITY QUESTIONNAIRE
FOR-PROFIT BUSINESS ENTITY**

Certification

The undersigned: (1) recognizes that this questionnaire is submitted for the express purpose of assisting New York State government entities (including the Office of the State Comptroller (OSC)) in making responsibility determinations regarding award or approval of a contract or subcontract and that such government entities will rely on information disclosed in the questionnaire in making responsibility determinations; (2) acknowledges that the New York State government entities and OSC may, in their discretion, by means which they may choose, verify the truth and accuracy of all statements made herein; and (3) acknowledges that intentional submission of false or misleading information may result in criminal penalties under State and/or Federal Law, as well as a finding of non-responsibility, contract suspension or contract termination.

The undersigned certifies that he/she:

- is knowledgeable about the submitting Business Entity's business and operations;
- has read and understands all of the questions contained in the questionnaire;
- has not altered the content of the questionnaire in any manner;
- has reviewed and/or supplied full and complete responses to each question;
- to the best of his/her knowledge, information and belief, confirms that the Business Entity's responses are true, accurate and complete, including all attachments, if applicable;
- understands that New York State government entities will rely on the information disclosed in the questionnaire when entering into a contract with the Business Entity; and
- is under an obligation to update the information provided herein to include any material changes to the Business Entity's responses at the time of bid/proposal submission through the contract award notification, and may be required to update the information at the request of the New York State government entities or OSC prior to the award and/or approval of a contract, or during the term of the contract.

Signature of Owner/Official _____

Printed Name of Signatory _____

Title _____

Name of Business _____

Address _____

City, State, Zip _____

Sworn to before me this _____ day of _____, 20____;

_____ Notary Public

Attachment 17

Encouraging Use of New York State Businesses in Contract Performance

Intentionally Blank

ENCOURAGING USE OF NEW YORK STATE BUSINESSES IN CONTRACT PERFORMANCE

New York State businesses have a substantial presence in State contracts and strongly contribute to the economies of the state and the nation. In recognition of their economic activity and leadership in doing business in New York State, bidders/proposers for this contract for commodities, services or technology are strongly encouraged and expected to consider New York State businesses in the fulfillment of the requirements of the contract. Such partnering may be as subcontractors, suppliers, protégés or other supporting roles.

Bidders/proposers need to be aware that all authorized users of this contract will be strongly encouraged, to the maximum extent practical and consistent with legal requirements, to use responsible and responsive New York State businesses in purchasing commodities that are of equal quality and functionality and in utilizing services and technology. Furthermore, bidders/proposers are reminded that they must continue to utilize small, minority and women-owned businesses, consistent with current State law.

Utilizing New York State businesses in State contracts will help create more private sector jobs, rebuild New York's infrastructure, and maximize economic activity to the mutual benefit of the contractor and its New York State business partners. New York State businesses will promote the contractor's optimal performance under the contract, thereby fully benefiting the public sector programs that are supported by associated procurements.

Public procurements can drive and improve the State's economic engine through promotion of the use of New York businesses by its contractors. The State therefore expects bidders/proposers to provide maximum assistance to New York businesses in their use of the contract. The potential participation by all kinds of New York businesses will deliver great value to the State and its taxpayers.

Bidders/proposers can demonstrate their commitment to the use of New York State businesses by responding to the question below:

Will New York State Businesses be used in the performance of this contract?
Yes No

If yes, identify New York State businesses that will be used and attach identifying information.

This Page Intentionally Blank

Attachment 18

Proposed Subcontractors

Intentionally Blank

Public Safety Credentialing and Training System RFP CJS 2014 01

Proposed Subcontractors

List each proposed subcontractor, as defined herein, proposed for use on the CJS 2014 01 project, in descending order (largest to smallest) of scope of services provided to project.

[illegible]

This Page Intentionally Blank

Attachment 19

Key Subcontractor Certification

Intentionally Blank

For each key subcontractor (as defined in the Glossary – Appendix Q) proposed by the Offerer in Attachment 20, submit a *Key Subcontractor Certification* that has been completed and executed by the proposed key subcontractor's authorized representative. Each proposed key subcontractor must complete and execute a *Key Subcontractor Certification* form.

An authorized representative of the Key Subcontractor who is legally authorized to certify the information requested in the name of and on behalf of the Key Subcontractor is required to complete and sign the Required Certifications. All of the requested information and certifications must be provided. Offerer's authorized representative must certify as to the truth of the representations made by signing where indicated, below.

CERTIFICATION:

The undersigned: (1) recognizes that these Required Certifications are submitted for the express purpose of assisting the State of New York in making a determination to award a Contract and/or approve a subcontract; (2) acknowledges and agrees by submitting the Certification, that the State may in its discretion, by means which it may choose, verify the truth and accuracy of all statements made herein; (3) acknowledges that intentional submission of false or misleading information may constitute a felony under Penal Law Section 210.40 or a misdemeanor under Penal Law Section 210.35 or Section 210.45, and may also be punishable by a fine of up to \$10,000 or imprisonment of up to five years under 18 USC Section 1001, and termination the Contract; and (4) certifies that the information submitted in this questionnaire and any attached pages is true, accurate and complete.

KEY SUBCONTRACTOR PROFILE			
Business Entity Name:			
Form of Legal Entity:	☐ Corporation ☐ Partnership ☐ Sole Proprietorship ☐ Other _____		
State of Incorporation:			
Main Office Address:			
Federal Tax ID #:			
NYS Certifications:	☐ Minority-Owned Business Enterprise (MBE)	☐ Women-Owned Business Enterprise (WBE)	☐ Small Business Enterprise (SBE)
Name & Title of Contact Person Authorized to represent Offerer in all matters relating to the submission of this Bid Proposal:	Signature: _____		
	Print Name: _____		
	Print Title: _____		
	Date: _____		
Address:			
Phone:			
Fax:			
E-Mail:			

NONDISCRIMINATION IN EMPLOYMENT IN NORTHERN IRELAND

[MACBRIDE FAIR EMPLOYMENT PRINCIPLES]

In accordance with New York State Finance Law, Section 165, the Key Subcontractor certifies that it or any individual or legal entity in which the Key Subcontractor holds a 10% or greater ownership interest, or any individual or legal entity that holds a 10% or greater ownership interest in the Contractor/Key Subcontractor, either (answer yes or no to one or both of the following, as applicable):

(1) have business operations in Northern Ireland,
No _____ Yes _____, and if yes:

(2) shall take lawful steps in good faith to conduct any business operations in Northern Ireland in accordance with the MacBride Fair Employment Principles relating to nondiscrimination in employment and freedom of workplace opportunity regarding such operations in Northern Ireland, and shall permit independent monitoring of compliance with such principles.
No _____ Yes _____

|
By: _____
Signature of Authorized Representative

Name: _____

Title: _____

Date: _____

Attachment 20

Draft Contract with Mandatory terms and Conditions

Intentionally Blank

DRAFT

New York State _____

-and-

[Contractor]

AGREEMENT

New York State Comptroller's Agreement Number _____

THIS AGREEMENT ("Agreement") is made this ____ day of _____ 2014 by and between the State of New York ("State"), acting through _____, an Executive Agency of the State of New York, with offices located at _____, and [Contractor], with offices located at _____. Contractor and _____ are collectively referred to hereinafter as the "Parties."

WHEREAS, DCJS is an Executive agency of the State of New York and has as one of its core business functions developing, acquiring, and procuring information technology and expert technology services to support its agency mission and the mission of New York State's Criminal Justice agencies through provision of integrated information technology support to law enforcement and maintaining a registry for police and peace officers of the State of New York; and

WHEREAS, the New York State Division of Criminal Justice Services (DCJS) solicited proposals by publication of a Request for Proposal (RFP) for development of a multi-purpose Public Safety Credentialing and Training System ("PSCTS") registry system for purposes of assisting interested state agencies in automating registration, credentialing, and training as to agency employees and/or those licensed or otherwise regulated by their respective agencies in New York State; and

WHEREAS, the first enumerated PSCTS Project to be undertaken under this RFP is with respect to a registry system for peace and police officers and security guard records maintained by DCJS; and

WHEREAS, in response to and in compliance with the RFP requirements, [Contractor] submitted its proposal and was selected by the State as the winning bidder; and

WHEREAS, the Parties now wish to execute an Agreement to effect these purposes;

NOW THEREFORE, in consideration of the mutual covenants herein contained, the Parties do agree as follows:

1. This Agreement, including all appendices, attachments and exhibits, copies of which are attached and incorporated by reference as though set forth in their entirety herein, and any Statement of Work (SOW) issued hereunder, constitutes the entire Agreement between the Parties. To the extent that they conflict with the terms hereof, all prior agreements, representations, statements, negotiations and undertakings are superseded by this Agreement. All statements made by DCJS, _____ or the State shall be deemed to be representations and not warranties. This Agreement is subject to amendment(s) only upon mutual written consent of the Parties, and if required by the Comptroller of the State of New York, the approval by the Comptroller of the State of New York or staff of the Office of the State Comptroller designated for such purpose.
2. This Agreement shall incorporate all of the following appendices, attachments and exhibits as though set forth herein in their entirety. Only the documents expressly enumerated below or contained within those documents enumerated below shall be deemed a part of this Agreement, and references contained in those documents to additional documents not enumerated below or included in any enumerated document shall be of no force and effect. Conflicts between this Contract and other documents shall be resolved in the following Order of Precedence:

Order of Precedence:

- 1) Appendix A (Standard Clauses for NYS Contracts). The parties agree that this contract is governed by and incorporates all of the terms and conditions of the document identified as Appendix A – Standard Clauses for New York State Contracts dated January 2014 annexed hereto and which is incorporated into this Contract as though fully set forth in its entirety herein.
- 2) This Agreement;
- 3) The following Appendices and/or other attachments annexed to this Agreement:
 - The DCJS Public Safety Credentialing and Training System Request For Proposal, issued _____ 2014, CJS2014-01, and its Appendices and Attachments
 - Contractor's RFP Submission and all Attachments/Appendices related thereto and Contractor's Clarification (where applicable), including any supporting material and any subsequent Contractor responses to inquiries in connection with services and costs under the Project;
 - Appendix B General Specifications;
 - Appendix C MWBE Reports;
 - OSC Consultant Contractor Services Form A and Form B Addendum;
 - MacBride Fair Employment – Northern Ireland Non-Discrimination;
 - Non Collusive Bidding Certification (State Finance Law Section 139-d);
 - DCJS Procurement Lobbying Guidelines;

- State Finance Law Sections 139-j and 139-k Affirmation;
 - Affirmation of Understanding and Agreement pursuant to State Finance Law §139-j (3) and §139-j (6) (b);
 - Disclosure of Prior Non Responsibility Determination;
 - State Non-Disclosure Agreement
 - Workers Compensation coverage certificate;
 - Proof of Disability Benefits Insurance
OR Form CE-200 from Workers Compensation demonstrating relief from Workers Compensation/Disability (see www.wcb.ny.gov);
 - Minority and Women-Owned Business Enterprise (MWBE) and Equal Opportunities Requirements;
 - Any Change Request Order Form which is subsequently mutually entered into with respect to services during the terms of this Agreement;
 - Any Statement of Work (SOW) issued by _____ or the State to the Contractor under the terms of this Agreement from time to time;
3. This Agreement shall not be deemed executed until signed by both parties and approved by the Attorney General of the State of New York and the Comptroller of the State of New York or their respective staff designated for that purpose.

This Agreement shall commence upon the date of its approval by the New York State Comptroller (“Effective Date”) and shall continue for a period of ten (10) years with the option to renew. The State reserves the right to renew the Agreement, in whole or in part, for two additional five (5) year terms upon the conditions and at the rates set forth in the Agreement or subsequent amendments, and as afforded by the cost of living index. The pricing in effect as of the first day of the third year shall be established as the Contractor’s base year. Except as established in Price Protection and any SOW provisions of the RFP, the Agreement will be subject to amendment only upon mutual written agreement of the parties, which agreement may necessitate approval by the Attorney General and the Comptroller of the State of New York. The State shall have the right to renegotiate the terms and conditions of the Agreement in the event applicable State or Federal law, policy, rules, regulations and guidelines are altered from those existing at the time of the original contractual agreement in order to be in continuous compliance therewith.

4. It is further understood and agreed that the Parties may implement certain changes between them in the details of this Agreement by executing a Change Request Order Form, a copy which is annexed herein as part of this Agreement. The Change Request Order Form must be mutually agreed to and executed by both parties, subject to approval by the New York State Office of Comptroller and any applicable control agency, if required, and when so executed shall be incorporated into this Agreement.

5. Any Statement of Work (SOW) shall contain specific deliverables and any sub-deliverables, and relevant completion date(s) and is subject to modification at the discretion of _____ or another State entity after consulting with the Contractor regarding reasonable service delivery performance. All such SOWs shall be signed by each party and take effect as indicated in such respective SOWs.
6. The costs of services rendered under this Contract shall be consistent with the Contractor's RFP Submission, and where applicable any subsequent Contractor service cost submission approved by _____ or any other State agency, including but not limited to any Change Request Order executed by both parties. The Contractor will provide additional optional services, as requested by _____ or any State agency procuring PSCTS project services, in accordance with the RFP and this Agreement. It is further agreed by Contractor that all of the prices, terms, warranties and benefits established in the Agreement are comparable to or better than the equivalent terms being offered by the Contractor to other customers using similar scope and volume of services. If the Contractor shall, during the term of this Agreement, enter into arrangements with any other customer providing greater benefits or more favorable terms, the Contract shall thereupon be deemed amended to provide the same to the State.
7. It is understood and agreed that the RFP enumerates specific Project-related roles and responsibilities of the Contractor and _____ and/or the State with respect to PSCTS project services. These include, but are not limited to the following:

Roles and Responsibilities of Contractor:

- a) Contractor staff will communicate directly with the assigned State agency Project Manager as the primary point of contact. A State agency may at its option change the designated assigned manager from time to time.
- b) Contractor will provide appropriate staff resources for any PSCTS project, including but not limited to having a representative on-site for all phases of system installation.
- c) Contractor staff will provide all requisite reports to the State as delineated in the RFP or this Agreement.
- d) All Contractor staff assigned to work with _____ or another State agency on any project related to their respective agency will be subject to approval by such State agency.
- e) Contractor shall provide written status and progress reports in a form to be agreed upon between the State and the Contractor and the Contractor shall provide a formal written report as otherwise specified in the RFP terms and conditions or as provided in the Scope of Work contained within any Task Order issued hereunder.

- f) Consultants and Contractors and certain of their Subcontractors who access DCJS, _____, and/or another State agency information, facilities or networks for which DCJS or said State agency maintains security controls may be subject to fees related to a fingerprint-based criminal history check and other necessary clearances.
- g) Contractor is responsible for maintaining and supporting any PSCTS project in accordance with the terms and conditions of the aforementioned RFP, this Agreement, any mutually executed Change Request Order or SOWs entered into. Contractor's initial PSCTS project services are with DCJS. Technical specifications regarding project services are contained in Section 3 of the RFP. The Contractor agrees to deliver support of software and any related databases via internet, telephone, e-mail and on-site visits as may be necessary. This support shall further include but not be limited to the following:
 - i. Software bug fixes
 - ii. Technical support related to problems or questions with the software.
 - iii. Enhancements, upgrades, and new functionality developed
 - iv. Support of upgrades and rollout of new software upgrades.
 - v. Maintaining the operational quality of the software.
 - vi. Provide technical support for required set-up and administration of server software as directed by the State.
- h) Contractor will provide software support by knowledgeable technical staff, as specified by the terms and conditions of the aforementioned RFP, which shall be at a minimum between the hours of 6:00 am to 6:00 pm Eastern Standard Time, Monday through Friday.
- i) Contractor shall timely respond to the State's support-related questions as specified within the Section 3.0 of the RFP.
- j) Contractor will maintain a sufficient level of trained and knowledgeable staff to be able to respond in a timely manner for requests from the State for billable services which may include refinement of software, training, implementation support, and miscellaneous problem solving.

Roles and Responsibilities of _____ or other authorized State agency:

- a) Provide an individual identified as the point of contact for Contractor's staff.
- b) Provide appropriate facility and software access at the project start consistent with the duties that will be performed. Contractor will safeguard all security passes and passwords, and return them at the completion of the engagement.
- c) Provide guidance and direction in the specific tasks to be performed.

- d) Provide appropriate staff resources to work with the Contractor as required and directed by applicable State agency management.
8. Comply with reasonable additional safeguards against improper disclosure, duplication, or use of Contractor's Confidential Information that Contractor may request from time to time, provided that these safeguards are not inconsistent with State law.
9. It is agreed that payments are to be made by _____ or any other applicable State agency in accordance with the terms and conditions of the payment schedule outlined in Section 3.2 of the RFP and Contractor's RFP response, or as otherwise mutually agreed by the parties. Contractor shall submit any invoices associated with a specific project deliverable at the completion of that activity. All payments from the State shall be made: (i) upon certification by the applicable State Agency Project Director or other designated State employee that the work invoiced by such invoice has been satisfactorily performed pursuant to the terms of this Contract, and (ii) upon submission of invoices satisfactory to the Comptroller of the State of New York in compliance with State Finance Law requirements.

Contractor shall provide complete and accurate billing invoices to the applicable State agency in order to receive payment. Billing invoices submitted to the agency must contain all information and supporting documentation required by the Agreement, the State agency and the State Comptroller. Payment for invoices submitted by the Contractor shall only be rendered electronically unless payment by paper check is expressly authorized by the head of such State agency, in his/her sole discretion, due to extenuating circumstances. Such electronic payment shall be made in accordance with ordinary State procedures and practices. The Contractor shall comply with the State Comptroller's procedures to authorize electronic payments. Authorization forms are available at the State Comptroller's website at www.osc.state.ny.us/epay/index.htm, by email at epayments@osc.state.ny.us, or by telephone at 518-474-4032. Contractor acknowledges that it will not receive payment on any invoices submitted under this Agreement if it does not comply with the State Comptroller's electronic payment procedures, except where the head of the State agency has expressly authorized payment by paper check as set forth above. It is further understood that the State shall only make payment upon the signed acceptance of project scheduled deliverables by an authorized State agency representative.

10. All Contractor personnel performing under this project, and all Contractor equipment used to process or store State data or to connect to network, must comply with the requirements contained in:
- a. The NYS Information Security Policy (P03-002) <http://www.dhses.ny.gov/ocs/resources/documents/cyber-security-policy-p03-002-v3.4.pdf>
 - b. NYS information technology policies, standards and best practice guidelines <http://www.its.ny.gov/tables/technologypolicyindex.htm> and

- c. State information security policies, procedures and standards. New York State law protects the privacy of criminal history and Sex Offender Registry records and other confidential information, including but not limited to certain employment, licensing, or registration records. Contractors shall take all reasonable steps required by the State to protect confidential information. This may include, but not be limited to, execution of a non-disclosure Agreement(s) with each individual assigned to provide work, background checks, fingerprint checks of Contractor and Subcontractor personnel with access to such information and a requirement that the Contractor and/or Subcontractor replace personnel at the discretion of the State.
- d. As enumerated in more detail in this Agreement, the Contractor must adhere to the "Information Security Breach and Notification Act" as set forth in State Technology Law Section 208 and General Business Law Article 39-F. The Contractor shall promptly notify the State where there is a reasonable belief of a breach of security, unauthorized access or unauthorized release of personal computer data containing personal information, and take appropriate action with respect to notification of the affected individuals and to other required state agencies consistent with the New York State Information Security Breach and Notification Act.

11. Contractor agrees to maintain the confidentiality of all information concerning any State agency operations, procedures, policies, and systems. In addition to this Agreement and any SOW, the Contractor and any authorized Subcontractor and the individuals assigned to work on this project, must agree to sign a Non-Disclosure Agreement with DCJS, _____ and/or any other State agency and to abide by all of the requirements therein.

12. _____ or the State will comply with reasonable additional safeguards against improper disclosure, duplication, or use of Contractor's Confidential Information that Contractor may request from time to time, provided that these safeguards do not interfere with or increase the cost of _____ or the State's use of the work product produced hereunder.

13. Contractor acknowledges that _____ and the State are subject to public disclosure laws and that this Agreement is a public record. Any specific information that is claimed by Contractor to be confidential or proprietary, shall be clearly identified as such by Contractor, and to the extent consistent with its public records laws, _____ and the State shall maintain the confidentiality of all such information marked confidential or proprietary. If a request is made to view Contractor's proprietary information, _____ or any other State agency procuring project services must notify Contractor of the request and of the date that such records will be released with sufficient time to allow Contractor to obtain a Court Order enjoining that disclosure. If Contractor fails to obtain a court order enjoining disclosure, _____ or the State may release the requested information on the date previously specified.

14. Other Terms and Conditions

The Contractor has agreed to abide by all RFP terms and conditions, including, but not limited to, specific provisions set forth below:

Governing Law

The laws of the State of New York shall govern this procurement and the Contract and all subcontracts issued hereunder. Actions or proceedings arising there from shall be heard in a court of competent jurisdiction in the State of New York. The terms of Appendix A, *Standard Clauses for New York State Contracts*, are expressly incorporated in this solicitation and the Contract as though set forth in their entirety herein.

Substantial/Material Change

The provisions of the State Finance Law §138 mandate the State's approval of subcontractors. Throughout the Contract term, in the event that there is a substantial or material change in the ownership or financial viability of the Contractor, its corporate affiliates, subsidiaries or divisions, or that of any key subcontractors as defined herein, the Contractor is required to provide notice and details of any such change to said contracting State agency in writing immediately when such is first known by Contractor, its corporate affiliates, subsidiaries or divisions, or key subcontractors.

"Substantial" or "material" change shall be defined to include, but not be limited to, sale, acquisitions, mergers or takeovers involving the Contractor, its corporate affiliates, subsidiaries or divisions, or key subcontractors which result in a change in the controlling ownership or assets of such entity after the submission of the Bid Proposal; or entry of an order for relief under Title 11 of the United States Code; the making of a general assignment for the benefit of creditors; the appointment of a general receiver or trustee in bankruptcy of Contractor's, its corporate affiliates, subsidiaries or divisions, or key subcontractors and partners' business or property; or action by Contractor, its corporate affiliates, subsidiaries or divisions, or key subcontractors and partners under any state insolvency or similar law for the purposes of its bankruptcy, reorganization or liquidation; or court ordered liquidation against Contractor, its corporate affiliates, subsidiaries or divisions, or key subcontractors and partners.

Upon receipt of such notice, any contracting State agency shall have a minimum of thirty (30) business days from the date of notice to review the information. The Contractor may not transfer the Contract among corporate affiliates, subsidiaries or divisions without the advance written consent of said State Agency and the New York State Office of State Comptroller, where applicable. In addition to any other remedies available at law or equity, the State agency shall have the right to prospectively cancel the Contract, in whole or in part for cause if it finds that such change materially and adversely affects the security, completion or ongoing operation of the PSCTS, solely determined with reference to the best interests of the State and the Authorized Users of the PSCTS.

Changes in Contractor's Project Team

Contractor will provide thirty (30) business days advance notice to the State in the event of a proposed change in the Project Team, or any key subcontractors named in the Bid Proposal. Such changes must be approved in writing in advance by the State. Upon the State's receipt of such notice, the State shall have thirty (30) business days from the date of notice to review the information. In addition to any other remedies available at law or equity, the State shall have the right to prospectively cancel the Contract, in whole or in part for cause if it finds that such change materially and adversely affects the security, completion or ongoing operation of the PSCTS, solely determined with reference to the best interests of the State. During the Contract term, the State agrees that it will not unreasonably withhold its consent to subcontractors. If exigent circumstances are present, the State will give the Contractor written notice of such circumstances requiring extension and the Parties may thereafter extend the thirty (30) business days for an additional thirty (30) business days in order to complete its review.

Third Party Beneficiary Requirement

Unless waived by the State, all subcontracts between the Contractor and a key subcontractor shall expressly name the State of New York as an intended third party beneficiary of such contracts.

Qualified Project Personnel

Personnel providing services on this project must be licensed or certified professionals where required by law. The Contractor must certify that equipment and service technicians are trained and qualified for the work being performed by the manufacturer of the proposed equipment, database management or software application developers. In the event that the Contractor identifies personnel for assignment to this project to the State in its proposal, the Contractor agrees not to reassign such identified personnel away from the project without the consent of the State, which consent shall not be unreasonably withheld.

Quality of Service

Should it be found that the quality of services being performed by the Contractor under the Contract, in whole or in part, are not in compliance with the Contract service requirements, the State may declare Contractor in default in accordance with the *Termination* section herein.

Ongoing Reports/Documentation

The Contractor shall provide project reports/documentation as a condition precedent to payment under the Contract. Failure to provide a report required within the due date may subject the Contractor to other actions determined appropriate by the State set forth herein. Upon notice, the Contractor shall have an opportunity to cure the default or be subject to Contract termination.

The State's failure to demand or receive required documentation shall not be deemed a waiver of rights under this paragraph.

All reports shall be delivered electronically. The parties to the Contract shall agree to an electronic format (e.g., application and required data elements) for any reports. Each report shall be transmitted to the applicable State agency electronically via the internet utilizing encryption standards and protocols approved by the State, where applicable, and the system used shall generate an electronic ticket acknowledging transmission.

All weekly reports required under this Section shall be due within two (2) business days after the last day of the required reporting period. All other reports which may be required under this RFP shall be due within ten (10) business days after the designated reporting period established by the State.

PSCTS Design, Conversion and Build Reports

During the Design, Conversion and Build Phase, the Contractor will provide the State with weekly reports of all activities to date. Such reports to include, but not be limited to:

1. Database Design, Conversion progress, testing of proposed schema
2. Selection and reporting of subcontractors
3. Progress reports on test system production systems
4. System Testing Reports from Contractor testing
5. Acceptance Testing Results
6. Integration Plan including Plans for Transition/Cutover
7. Progress of All Work
8. Updated, As-Built Design Drawings

The Contractor shall hold a series of walkthroughs of its documentation for the State in advance of critical milestones. Materials to be reviewed at each walkthrough shall be delivered to the State at least two (2) weeks prior to the scheduled date of the walkthrough. Prior to System Implementation, the Contractor shall provide documentation about scalability, interoperability, performance and security of the proposed system for review by the State Architecture team. System Implementation shall not take place without approval of this material by the State Architecture team.

Insurance and Maintenance Bond

A. General

The Contractor shall file with the _____, Certificates of Insurance evidencing compliance with all requirements contained in this RFP no more than thirty (30) calendar days after receipt of "Notice of Contract Award" from the State and annually thereafter to any contracting State agency. Such Certificates of Insurance shall be of form and substance acceptable to the State. Acceptance and/or approval of the State of the Certificates of Insurance does not and shall not be construed to relieve the Contractor of any obligations, responsibilities or liabilities under the Contract. All insurance required by the Contract shall be

for the performance of the Contractor's obligations during the term of this Contract, and shall be obtained at the sole cost and expense of the Contractor, and shall be maintained with insurance carriers licensed or authorized by the New York State Department of Financial Services to issue insurance in the State of New York; In addition, all such insurance policies shall provide that the required coverage shall apply on a primary and not on an excess or contributing basis as to any other insurance that may be available to _____ and/or the State of New York for any claim arising from the Contractor's work under this Contract, or as a result of the Contractor's activities. Any other insurance maintained by _____ or the State of New York shall be excess of and shall not contribute with the Contractor's insurance regardless of the "other insurance" clause contained in _____ or the State's own policy of insurance. Further, Contractor's insurance policies, unless otherwise mutually agreed by the State, shall be endorsed to provide that written notice must be given to any contracting State agency at least thirty (30) calendar days prior to cancellation, non-renewal, or material alteration of such policy or policies, which notice, evidenced by return receipt of United States Certified Mail shall be sent to the applicable State agency Project Manager. The insurance policies shall name the State of New York, its Officers, agents and employees as additional insured's thereunder.

B. Payment of Premium & Deductible

The Contractor shall be solely responsible for the payment of all premiums and deductibles to which all such policies are subject, and the State shall have the right, in the event of a default or other failure by the Contractor to make a premium or deductible payment associated with the coverage's set forth in this section, to pay the required premium(s) or to settle the outstanding balance due with a carrier and to deduct the cost therefore from any sums otherwise due the Contractor under the agreement.

C. Carrier(s)

Insurance shall be maintained with insurance carriers licensed to do business in New York State. Each insurance carrier must be rated with an A.M. Best Company rating of "A-" Class "VII" or better in the most recently published Best's Insurance Report. If, during the term of the policy, a carrier's rating falls below "A-" Class "VII," the insurance must be replaced no later than thirty (30) calendar days from the date of the negative rating change or the renewal date of the policy, whichever occurs sooner, with an insurer acceptable to the State and rated at least "A-" Class "VII" in the most recently published Best's Insurance Report.

D. Coverage Term

The Contractor shall cause all insurance to be in full force and effect as of the date that the Contract resulting from this RFP is approved by the Office of the State Comptroller and to remain in full force and effect throughout the term of the Contract and as otherwise required by the terms and conditions of the Contract. The Contractor shall not take any action, or omit to take any action, that would suspend or invalidate any of the required coverage's during the period of time such coverage's are required to be in effect. Not less than 30 calendar days prior to the

expiration or renewal date the Contractor shall supply the State updated replacement Certificates of Insurance, and amendatory endorsements.

E. Form of Insurance

The required insurance certificates shall: (1) name the People of the State of New York, its officers and agents as additional insureds, (2) be in a form and substance acceptable to the State; (3) be obtained at the sole cost and expense of the Contractor; (4) be maintained with insurance carriers licensed or otherwise authorized to do business in New York who are acceptable to the State; (5) be primary and non-contributing to any insurance or self-insurance maintained by the State; (6) contain the standard ISO separation-of-insureds provision, or a substantially similar clause; (7) be endorsed to provide written notice to the State at least 30 calendar days prior to the cancellation, non-renewal, or material alteration of such policies, which notice shall be evidenced by return receipt of United States Certified Mail sent to the attention of:

CONTACT INFORMATION TO BE IN FINAL CONTRACT

and where applicable, to the address of any other contracting State agency. In no event shall any certificate form's cancellation provision, contain the words "endeavor to" and/or "but failure to mail such notice shall impose no obligation or liability of any kind upon the company, its agents, or representatives" or similar language within its provisions.

F. Subcontractor Insurance

Additionally, the Contractor shall require all of its subcontractors performing work in connection with the Contract, prior to commencement of an agreement between Contractor and the Subcontractor, to secure and keep in force during the term of their contractual services, the applicable insurance requirements of this section. Satisfactory proof thereof shall be supplied by the Contractor to _____ or where applicable to such other State official or employee designated by the State upon request.

G. Right to Make Claim

The failure of: (1) the Contractor to furnish certificates that comply with the requirements of the Contract, or (2) the State to demand such certificate or other evidence of full compliance with these insurance requirements, or (3) the State to identify a deficiency from evidence that is provided to the State, or (4) the State to make payment on behalf of the Contractor in order to maintain required coverage's, shall not be construed as a waiver of the State right's to enforce the provisions of this section, or as a waiver of the Contractor's liability for failure to meet the insurance requirements set forth herein. In addition to any other legal or equitable remedies that may be available to the State, failure to maintain the required insurance may, in the State's sole judgment, be grounds for a termination of the Agreement for cause. By requiring insurance, the State does not represent that coverage and limits will necessarily be adequate to protect the State and such coverage and limits shall not be deemed as a limitation on the Contractor's liability to the State under the Contract.

H. Commercial General Liability & Umbrella Liability Insurance

The Contractor shall maintain commercial general liability (CGL) and, if necessary, commercial umbrella insurance with a limit of not less than two million dollars annually for each occurrence which shall be effective as of the date of approval of the contract by the New York State Comptroller. Such liability shall be written on ISO occurrence form CG 00 01 01 96(or a substitute form providing equivalent coverage) and shall cover applicable liability arising from premises, operations, independent contractors, subcontractors, all product (including any equipment and system components) completed operations during the contract period, broad form property damage, personal injury, defense and/or indemnifications obligations, including obligations under any resulting Contract, cross liability coverage and liability assumed in a contract (including the tort liability of another assumed in a contract). The State shall be included as an insured under the CGL, using ISO additional-insured endorsement (General Liability Additional-Insured Endorsement shall be on Insurance Service Office's (ISO's) form number CG 20 10 11 85) or a substitute providing equivalent coverage, and under the commercial umbrella, if any. This insurance shall apply as primary insurance with respect to any other insurance or self-insurance programs afforded to the State. The Contractor shall submit insurance verification information acceptable to the State upon request.

I. Comprehensive Professional Liability Insurance

If providing professional services, the Contractor shall maintain, or if subcontracting professional services, shall certify that Subcontractor maintains errors and omissions liability insurance with a limit of not less than one million dollars per loss annually. Such insurance shall apply to professional errors, acts, or omissions arising out of the scope of services covered by this Contract and may not exclude bodily injury, property damage, testing, monitoring, measuring, or laboratory analyses, where applicable. If coverage is written on a claims-made policy, the Contractor warrants that any applicable retroactive date precedes the effective date of this Contract; and that continuous coverage will be maintained throughout the contract.

J. Liability Insurance Policies/State Designation

Any aforementioned Insurance Policies issued must be in the name of "The People of the State of New York", with appropriate dollar coverage.

K. New York State Worker's Compensation Law

Sections 57 and 220 of the New York State Workers' Compensation Law (WCL) provide that the State shall not enter into any contract unless proof of workers' compensation and disability benefits insurance coverage is produced. Prior to entering into a contract with the State, any successful Contractor will be required to verify for the State, on forms authorized by the New York State Workers' Compensation Board, the fact that they are properly insured or are otherwise in compliance with the insurance provisions of the WCL. The forms to be used to show compliance with the WCL are listed below.. Any questions relating to either workers'

compensation or disability benefits coverage should be directed to the State of New York Workers' Compensation Board, Bureau of Compliance at 1-866-298-7830. Failure to provide verification of either of these types of insurance coverage throughout the contract term to the State is grounds for termination of the contract.

Workers' Compensation Requirements under WCL § 57:

To assist state and municipal entities in enforcing WCL §57, businesses requesting permits, licenses or seeking to enter into contracts must provide ONE of the following forms to the entity issuing the permit or entering into a contract:

- Certificate of Attestation of Exemption from NYS Workers' Compensation and/or Disability Benefits Coverage (CE-200); or
- Certificate of Workers' Compensation Insurance (C-105.2) (the business' insurance carrier will send this form to the government entity upon request) Please Note: The State Insurance Fund provides its own version of this form, the U-26.3; or
- Certificate of Worker's Compensation Self-Insurance (SI-12) (the business calls the Board's Self- Insurance Office at 518-402-0247); or
- Certificate of Group Worker's Compensation Self-Insurance (GSI-105.2) (the business' Group Self- Insurance Administrator will send this form to the government entity upon request).

Effective September 9, 2007, all out-of-state employers with employees or subcontractors working in New York State are required to carry a full, statutory New York State workers' compensation insurance policy.

An employer has a full, statutory New York State workers' compensation insurance policy when New York is listed in Item "3A" on the Information Page of the employer's workers' compensation insurance policy. Please contact the Board's Bureau of Compliance at 1-866-298-7830 if you have any questions regarding these requirements.

Please note: If all work for the permit, license or contract is done outside of New York and no employees of the out-of-state business work in the state, New York State-specific coverage is not required and the employer may be able to file Form CE-200.

Disability Benefits Requirements under WCL § 220(8):

To assist state and municipal entities in enforcing Sec. 220 Subd. 8 of the New York State Disability Benefits Law, businesses requesting permits, licenses or seeking to enter into contracts must provide one of the following forms to the government entity issuing the permit, license or entering into a contract:

- Certificate of Attestation of Exemption from NYS Workers' Compensation and/or Disability Benefits Coverage (CE-200); or
- Certificate of NYS Disability Benefits Insurance (DB-120.1) (the business' disability benefits carrier will send this form to the government entity upon request)
- Certificate of NYS Disability Benefits Self-Insurance. (DB-155) (businesses that are self-insured in NYS for disability benefits insurance should call the Workers' Compensation Board's Self-Insurance Office at (518) 402-0247 to obtain this form.)

Please note: New York State statutory disability benefits (DB) insurance coverage is totally different from and is not included in New York State workers' compensation insurance coverage. Statutory New York State disability benefits insurance covers employees for an off-the-job accident, injury or illness and pays half an employee's weekly wage, up to \$170 per week, for up to 26 weeks.

An out-of-state employer needs a New York State disability benefits insurance policy if the employer employs one or more individuals on each of at least 30 days in a calendar year in New York State. To be eligible for a disability benefits exemption using Form CE-200, an out-of-state employer must not have one or more individuals working on each of at least 30 days in a calendar year in New York. (Independent contractors are not considered to be employees under the Disability Benefits Law.)

If you have any additional questions regarding workers' compensation coverage requirements, please call the Bureau of Compliance at (866) 298-7830.

Obtaining Workers' Compensation and Disability Benefits Insurance

It may be appropriate to check the yellow pages, contact your insurance broker, carrier or agent, check with your trade association, or conduct additional research to find the most appropriate insurance coverage for your company. In addition, a workers' compensation policy may be obtained from the NYS Insurance Fund by calling 1-888-875-5790 and a disability benefits insurance policy may be obtained from the NYS Insurance Fund by calling 1-866-697-4332.

Maintenance Bond

The Contractor shall post and keep in effect throughout the term of the Contract, a faithful performance bond to secure the maintenance and repair responsibilities required by the Contract and by agreements for Authorized User locations under the jurisdiction of the Contract.

For each year that the Contractor is obligated to perform maintenance, the bond shall be furnished in a sum equal to a mutually agreeable reasonable estimate of the Contractor's annual maintenance and repair responsibilities based upon the annual maintenance plan furnished at the commencement of the Contract. The Contractor's initial Annual Maintenance Plan and estimate of annual maintenance costs for the PSCTS are set forth in Attachment 24.

The maintenance bond shall be from a surety and in a form that has been approved in advance, by the State and shall name the State as an irrevocable beneficiary of any portion or the full amount which will entitle the State to proceed against the bond upon the failure of the Contractor to provide the planned and unplanned maintenance required under this Contract. A copy of the maintenance bond shall be promptly forwarded to _____ and/or other designated State officials.

Title & Legal Interests

A. Documentation

The State shall own title to all drawings, documentation, technical designs and specifications (including but not limited to bid proposals, engineering drawings, plans, reports, training, maintenance or operating manuals), including network design, equipment configurations and documentation, whether preliminary, final or otherwise and may reproduce same for its own use. The Contractor shall deliver to the possession of _____ or any other applicable State agency all work-in-progress documentation as it becomes available, but in no event later than thirty (30) calendar days after creation.

B. Incorporation into Subcontracts

The Contractor shall incorporate all of the provisions hereof respecting Title and Legal Interests in Documentation, and PSCTS Infrastructure into subcontracts entered into by the Contractor in connection with performance of Contractor's obligations under the terms of this RFP and resulting Contract. Other than as set forth above and with express written approval of the State, the Contractor shall not sell, assign, encumber, lien or otherwise pledge PSCTS Infrastructure as collateral for any obligations or indebtedness of the Contractor.

Warranties

In addition to the warranties set forth elsewhere in the Contract, the following warranties **shall survive beyond termination or expiration of the Contract** term in accordance with the terms below. Contractor, in submitting its Bid Proposal and executing the Contract, warrants and represents to the State the following:

A. PSCTS Performance

Contractor warrants that all components or deliverables specified and furnished by or through the Contractor under this Contract meet the requirements set forth in the RFP and any subsequent Statement(s) of Work (SOW), and that services will be provided in a workmanlike manner in accordance with industry standards warrants and represents that the PSCTS shall operate in accordance with the requirements and acceptance criteria set forth in the Contract. If any portion of the PSCTS fails to meet this warranty standard, the Contractor shall repair or replace the defective component at its sole expense to minimize disruption and loss of functionality, time being of the essence.

Contractor warrants and represents full ownership, clear title free of all liens, and/or that Contractor has obtained on behalf of and thereafter to any other State agency providing PSCTS services a perpetual license rights set forth herein to use the Contractor's proposed PSCTS solution including equipment, software, customizations and services ("Product"), for the purposes stated in Section 1.4 of the RFP. Contractor shall indemnify any contracting State agency and the State for any loss, damages or actions arising from a breach of this warranty without limitation. The State may require Contractor to furnish appropriate written documentation establishing the above rights and interests as a payment. The State's request or failure to request such documentation shall not relieve Contractor of liability under this warranty.

Contractor warrants and represents that any required deliverables specified and furnished by or through Contractor, whether tangible or intangible, regardless of form, shall be standard new equipment, current model or most recent release of regular stock product with all parts regularly used with the type of equipment offered, with no attachment or part substituted or applied contrary to the manufacturer's recommendations and standard commercial practice in the industry.

Contractor warrants and represents that all Products or deliverables specified and furnished by or through Contractor under the Contract meet the completion criteria set forth in the Contract and any subsequent SOW, and that services will be provided in a workmanlike manner in accordance with industry standards, as applicable.

Contractor further warrants and represents that Products or deliverables specified and furnished by or through the Contractor under the Contract shall individually, and where specified by Contractor to perform as a system, be substantially uninterrupted and error free in operation and guaranteed against faulty material and workmanship for the warranty period stated in the Contract, or a minimum of eighteen (18) months from the date of acceptance, whichever period is longer ("Project Warranty Period"). During the Project Warranty Period, defects in the Products or deliverables specified and furnished by or through Contractor shall be repaired or replaced at no cost or expense to _____ or as applicable to any other State agency procuring PSCTS project services.

Contractor shall extend the Project Warranty Period for individual Product(s) or for the PSCTS as a whole, if applicable, by the cumulative period(s) of time, after notification, during which an individual Product or the PSCTS requires servicing or replacement (down time), or is in the possession of the Contractor's subcontractors, distributors, resellers or employees. In addition to Contractor's Project Warranty; _____ or any other State agency procuring PSCTS project services shall have the benefit of all manufacturers' standard commercial warranties for individual project deliverables. It shall be the Contractor's responsibility to insure such warranties begin conterminously with the commencement of Contractor's Project Warranty Period. Any additional cost(s) for having the periods begin conterminously shall be borne by the Contractor. During the Project Warranty Period, Contractor shall be responsible for placing and coordinating all manufacturers' warranty claims on behalf of

any applicable State agency. Such manufacturer's warranty coverage shall be supplemental to, and not relieve the Contractor from its warranty obligations during the Project Warranty Period.

Where the manufacturer's warranty term is longer than the Project Warranty Period, Contractor shall notify any applicable State agency and pass through the manufacturer's warranty to _____ and the State at no additional charge. Contractor shall not be responsible for coordinating services under the manufacturer's warranty after expiration of the Project Warranty Period.

B. Conformance to Manufacturer's Specifications

The warranties expressly set forth in this RFP and resulting Contract will be in lieu of all other warranties, express or implied including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The above warranties do not apply to the extent the problem is caused by misuse, unauthorized modification, unsuitable physical environment, failure to follow required maintenance by the State or failure caused by product for which the Contractor is not responsible.

C. Product & Equipment Warranty

At all times during the Contract term, Contractor warrants and represents that the Product delivered under this Contract conform to the requirements, specifications, performance standards and documentation, and the documentation fully describes the proper procedure for use. Technologies and equipment offered shall be standard new equipment, current model or most recent version or release of standard commercial offering with all parts regularly used with the type of equipment offered; and no attachment or part has been substituted or applied contrary to the manufacturer's recommendations and standard practice.

Contractor further warrants and represents that the Product delivered under this Contract (including any equipment, components or deliverables specified and furnished by or through Contractor) shall individually, and where specified and furnished as a system, be substantially uninterrupted or error-free in operation and guaranteed against faulty material and workmanship for the manufacturer's standard warranty period or for the duration of the Contract, whichever is longer ("warranty period"). During the warranty period, defects in the materials or workmanship of components or deliverables specified and furnished by or through Contractor shall be repaired or replaced by Contractor at no cost or expense to the State.

If during the warranty periods faults develop, the Contractor shall promptly repair or, upon demand, replace the defective unit or component part affected. Substituted or replacement Product shall be unconditionally guaranteed for a period of one year from the date such substituted or replacement Product was installed or replaced, the standard manufacturer's warranty period, or the remaining duration of the warranty period, whichever is longer.

Where third party equipment manufacturer or software developer offers any project deliverable by or through Contractor with a standard commercial warranty, such standard warranty shall be

in addition to, and not relieve the Contractor from, Contractor's warranty obligations during the project warranty period(s). Where a standard commercial warranty covers all or some of the warranty period(s), Contractor shall be responsible for coordinating the warranty service with the third party manufacturer(s) or developers.

All costs for labor and material and transportation incurred to repair or replace defective Product during the warranty period shall be borne solely by the Contractor, and the State shall in no event be liable or responsible therefore.

D. Title & Ownership Warranty

Contractor warrants and represents full ownership, clear title free of all liens and encumbrances, and/or that Contractor has obtained on behalf of the State perpetual license rights to use the contracted PSCTS Product, hardware, interfaces, third-party software or any other deliverable ("System") pursuant to this Contract. Contractor shall be solely liable for any costs of acquisition associated therewith. Contractor fully indemnifies the State for any loss, damages or actions arising from a breach of said warranty without limitation. The State or _____ ("Authorized PSCTS User") may require Contractor to furnish appropriate written documentation establishing the above rights and interests as a condition of Contract award or payment. The State's request or failure to request such documentation shall not relieve Contractor of liability under this warranty.

E. Contractor Compliance

Contractor warrants and represents that it will pay, at its sole expense, all applicable permits, licenses, tariffs, tolls and fees and gives all notices and complies with all laws, ordinances, rules and regulations of any governmental entity in conjunction with the performance of obligations under the Contract. Prior to award and during the Contract term and any renewals thereof, Contractor shall establish to the satisfaction of the State that it meets or exceeds all requirements of the bid/ Contract and any applicable laws, including but not limited to, permits, insurance coverage, licensing, proof of coverage for workman's compensation, and shall provide such proof as required by the State. Failure to do so may constitute grounds for the State to cancel or suspend this Contract, in whole or in part, or to take any other action deemed necessary by the State.

F. Virus Warranty

Contractor warrants and represents that licensed or customized Software contains no known viruses.

G. Workmanship Warranty

Contractor warrants and represents that all components or deliverables specified and furnished by or through Contractor under the Contract meet the completion criteria set forth in the Contract and any subsequent statement(s) of work, and that services will be provided in a workmanlike manner in accordance with industry standards.

H. Adequate Parts Supply

Contractor warrants and represents that adequate parts supply will be available throughout the term of the Contract and extensions and stored in such locations to meet the response times and performance specifications set forth herein.

I. Date Processing Warranty

Contractor warrants and represents that Contract services involving the processing of date/time data shall be provided in an accurate and timely manner insofar as accurately processing date/time data, including leap year calculations. In the event of any breach of this warranty, the Contractor shall restore the services to the same level of performance as warranted herein, and clean, repair or replace data, time being of the essence, at the Contractors' sole cost and expense.

The Contractor shall, at its sole cost and expense, promptly repair or, upon demand, replace the defective unit or component part affected or furnish a patch or temporary fix or work around during the period in which the repair is made so that the performance and functionality of the PSCTS is maintained, time being of the essence.

All costs for labor and material and transportation incurred to repair or replace defective equipment or components during the warranty periods shall be borne solely by the Contractor, and the State shall in no event be liable or responsible therefore.

The Contractor shall provide a warranty period of eighteen months from the date of system acceptance for all products and deliverables. This warranty period shall include full maintenance services at no additional cost to _____ or any other contracting State agency. The Contractor shall include details of the proposed warranty to meet _____ or another State agency's needs as described in this RFP.

J. Personnel Eligible for Employment

The Contractor further warrants to the State that contractor personnel performing services under the Contract are eligible for employment in the United States.

K. Survival of Warranties

All warranties contained in the Contract shall survive the termination of the Contract. The Contractor will maintain all original manufacturers' warranties and will present the organized warranty package to _____ and any other State official or employee upon completion and/or termination of contract, as requested.

Indemnification & Limitation of Liability

A. Contractor shall be fully liable for the actions of its agents, employees or subcontractors and shall fully indemnify and save harmless the State, DCJS, _____, and any other contracting State agency from suits, actions, damages and costs of every name and description for acts or omissions including but not limited to those relating to personal injury and damage to real or personal tangible property caused by Contractor, its agents, employees, subcontractors, *without limitation*; provided, however, that the Contractor shall not indemnify for that portion of any claim, loss or damage arising hereunder arising from the negligence of DCJS, _____, any other contracting State agency, or their respective State agency employees.

B. Contractor will indemnify, defend and hold _____, and any other contracting State agency, and the State harmless, *without limitation*, from and against any and all damages, losses, expenses (including reasonable attorneys' fees), claims, judgments, liabilities and costs which may be finally assessed against _____, any other State agency, and/or the State as a whole in any action for infringement of a patent with respect to the Product furnished, or of any copyright, trademark, trade secret or intellectual property right, provided that the Contractor receives: (i) prompt written notice of any action, claim or threat of infringement suit, or other suit, (ii) the opportunity to take over, settle or defend such action, claim or suit at Contractor's sole expense, and (iii) assistance in the defense of any such action at the expense of Contractor. Where a dispute or claim arises relative to a real or anticipated infringement, the Contractor may be required at its sole expense, to submit such information and documentation, including formal patent attorney opinions, as DCJS, _____ another State entity, including the Department of Law shall require. If the Contractor has an opportunity to terminate any such infringement suit by a third-party Contractor, the Contractor shall obtain State consent from DCJS, _____, any other contracting State agency, and the Attorney General of the State of New York to the settlement if such settlement will alter any financial or performance terms of the Agreement.

C. If principles of governmental or public law are involved, DCJS, _____ and the State may participate in the defense of any such action, but no costs or expenses shall be incurred for the account of the Contractor without its written consent.

D. If in the Contractor's opinion the equipment, materials, or information mentioned above are likely to or do become the subject of a claim of infringement of a United States patent or copyright, then without diminishing the Contractor's obligation to satisfy any final award, Contractor may, with DCJS, _____ and/or any other contracting State agency, and the State's written consent, substitute other equally suitable equipment, materials, and information or, at Contractor's option and expense, obtain the right for the State to continue the use of such equipment, materials, and information.

E The Contractor will indemnify DCJS, _____ other contracting State agency and the State *without limitation* against any claims brought against any such State agency and/or the State by

reason of a wrongful disclosure of confidential information attributed to the Contractor or any of its agents, employees, and/or subcontractors and will cooperate fully with DCJS, _____, the State, and the Attorney General in defense of any claim(s).

F. The Contractor shall not be obligated to indemnify that portion of a claim or dispute based upon: i) unauthorized modification or alteration of a product; ii) use of the product in combination with other products not furnished by Contractor; iii) use in other than the specified operating conditions and environment.

G. Neither party shall be liable for any delay or failure in performance beyond its control resulting from acts of God or force majeure. All parties shall use reasonable efforts to eliminate or minimize the effect of such events upon performance of their respective duties under the Contract and shall immediately resume performance upon termination of the force majeure.

H. Unless otherwise specifically enumerated herein, neither party shall be liable to the other for special, indirect or consequential damages, including lost data or records (unless the Contractor is required to back-up the data or records as part of the work plan), even if the party has been advised of the possibility of such damages. Neither party shall be liable for lost profits, lost revenue or lost institutional operating savings. Indemnification for Direct Damage: For all other claims against the Contractor where liability is not otherwise set forth in the Contract as being “without limitation” and regardless of the basis on which the claim is made, Contractor’s liability under this Contract for direct damages shall be two (2) times the charges rendered by the Contractor under the Contract.

I. DCJS, _____, another contracting State agency, and the State may, in addition to other remedies available to them at law, in equity, or under the Contract, and upon notice to the Contractor, retain such monies from amounts due Contractor, or may proceed against the maintenance bond, as may be necessary to satisfy any claim for damages, costs and the like asserted by or against them.

Software, Customizations Upgrades

Software error corrections, revisions, feature enhancements or upgrades for products delivered under this Contract, including the PSCTS, will be provided at no charge by the Contractor during the Contract term and shall be made available throughout the life of the Contract, including any contractual amendment, at no additional charge other than the pricing set forth in the Contract, unless otherwise agreed in writing by _____ or any other contracting State agency.

The Contractor will be required to notify any contracting State agency immediately of the availability of software upgrade(s). Implementation of an upgrade is at the sole discretion of the State, provided, however, that the non-implementation of any software upgrade does not substantially impair system performance or reliability.

A. Software License

Title and ownership to proprietary commercial software delivered under the Contract shall remain with the proprietary owner(s) ("Licensor"). Effective upon delivery, such software shall be perpetually licensed to the State. Licensor may not terminate the use of the Product in ways which would otherwise be prohibited by law ("License") without first providing any contracting State agency with written notice of the material breach giving rise to the termination and a thirty (30) calendar day opportunity to cure.

B. Archival Back-up for Licensed Software

The Contractor shall copy and retain the licensed software and related documentation for all software and upgrades for the purpose of 1) trouble shooting diagnostic; 2) reproducing copies of the Licensed Product for archival backup and disaster recovery procedures in the event of destruction or corruption of the software or disasters or emergencies which require PSCTS to restore backup(s) or to initiate disaster recovery procedures for its platform or operating systems; and 3) reproducing a reasonable number of copies of the Product and related documentation for cold site storage. "Cold Site" storage shall be defined as a restorable back-up copy of the Product not to be installed until and after the declaration by the State of a disaster.

C. Transfers or Assignments to a Third Party Agent

The State may assign or transfer its rights in licensed software to a third party entity or trustee ("Trustee").

D. Confidentiality/Licensed Software

Licensed software is considered a trade secret, copyrighted and proprietary product. The State will not disclose or otherwise distribute or reproduce any licensed software to anyone other than as authorized under the terms of Contract. The State will not remove or destroy any proprietary markings of Contractor. Except as expressly authorized by the terms of license, the State shall not:

1. Copy the Product;
2. Cause or permit reverse compilation or reverse assembly of all or any portion of the Product;
3. Export all or any portion of the Product in violation of any U.S. Department of Commerce export administration regulations.

Escrow for Software Source Code

Contractor shall establish and maintain, at its expense, an established escrow agreement in effect in perpetuity for the original installed and every subsequent version of the source code, including proprietary code, to the software delivered under the Contract ("Source Code"). The Contractor shall establish procedures to continually update the Source Code, including any change in the proprietary code, as new versions of the software are implemented into production.

A. Escrow

The Contractor shall provide in writing to ____DETAILS IN FINAL CONTRACT____ or such State official or employee designated for such purpose, the name and contact address/phone number of the neutral third party ("Escrow Agent") holding, in trust, all original installed and subsequent versions of the Source Code, including proprietary code, designated to the State. The escrow agreement has to name DCJS,____, or any other contracting State agency, as applicable, and the State of New York as an irrevocable beneficiary, and the State of New York acting on behalf of Authorized PSCTS User(s) of this Contract. The escrow agreement may not be terminated by either Contractor or the Escrow Agent without prior written approval by the State. Throughout the term of the Contract, Contractor shall be obligated to annually update and appropriately identify the deposited materials, including current versions of the source code for the most recent release, error corrections, enhancements or updates of software delivered under this Contract.

B. Terms of Escrow

The Contractor's Escrow Agent shall provide annual written notice to the State that such escrow is in effect, and shall notify in writing the State as to the version or releases held by such agent by providing the contents list for the escrow. The Escrow Agent shall, during the term of the escrow agreement, periodically inspect the deposit materials and compare them with the contents list for the escrow. The Escrow Agent may not raise any defenses against the State that the agent may have against the Contractor to restrict the release of source code to the State. The escrow agreement shall not include any provisions relating to the release of the escrow contents that would require, prior to release, the State to submit to arbitration. The escrow agreement shall require the Escrow Agent to provide the following notices and to release the escrow as follows:

(1). Required Notice to State from Escrow Agent:

The Escrow Agent is required to furnish written notice(s) to ____DETAILS IN FINAL CONTRACT____ (at the address for notices set forth in this RFP, Section 5.8.E), and to the designated person of any other State agency procuring PSCTS project services upon the happening of any one or more of the following events:

- a. Failure of Contractor to pay required escrow fees;
- b. Voluntary termination or transfer of escrow account by Contractor;
- c. Entry of an order for relief under Title 11 of the United States Code against Contractor, or any involuntary order;

- d. The making of a general assignment by Contractor for the benefit of creditors;
- e. The appointment of a general receiver or trustee in bankruptcy of Contractor's business or property;
- f. Action by Contractor under any state insolvency or similar law for the purposes of its bankruptcy, reorganization or liquidation;
- g. Court ordered liquidation against Contractor; or
- h. Contractor's failure to update the Source Code and/or to deposit new code with Escrow Agent at least annually after the effective date of the escrow.

(2). Requirement for Release of Source Code

The terms of escrow shall provide for release of the source code upon the happening of one or more of the following events:

- a. Failure of Contractor to carry out PSCTS ongoing maintenance or support obligations set forth in this Contract;
- b. Failure of Contractor to continue to do business in the ordinary course;
- c. Existence of any one or more of the following circumstances, if uncorrected for more than sixty (60) calendar days:
 - i. entry of an order for relief under Title 11 of the United States Code;
 - ii. the making by the Contractor of a general assignment for the benefit of creditors;
 - iii. the appointment of a general receiver or trustee in bankruptcy of Contractor's business or property; or action by the Contractor under any state insolvency or similar law for the purposes of its bankruptcy, reorganization, or liquidation.

The occurrence of the described events will not constitute a release condition if, within the specified sixty (60) calendar day period, Contractor (including its assignee or its receiver or trustee in bankruptcy) provides to the State adequate assurances, reasonably acceptable to the State as solely determined by State, of its continuing ability and willingness to fulfill all of its maintenance and support obligations. Additionally, if the State feels that a condition for release has occurred, the State shall notify the Escrow Agent, who shall notify Contractor of the intended release. Contractor has a maximum of fifteen (15) business days to object to the release. If an objection is filed, the Escrow Agent shall continue to retain the source code until otherwise directed by mutual agreement of the parties or until otherwise directed by a court of competent jurisdiction. Notwithstanding the foregoing, if after an objection has been filed, the State certifies in writing an "emergency", as defined below, has occurred, the Escrow Agent shall immediately release the source code to the State. An "emergency" shall be defined as the State's written certification that, the State reasonably believes that a feature in the Contractor's product has caused the system to crash and render it inoperable and the Contractor has refused to provide remedial assistance to correct the failure within five (5) business days from receipt of written notice, via e-mail, of the failure and such condition requires an immediate release of the source

code for State's internal use to correct the failure in order to continue normal system operation and full functionality. Upon release of the Source Code, the State may release the Source Code to the Authorized PSCTS User(s), if necessary, for remedial maintenance purposes only.

C. Changes in Escrow

The escrow agreement shall designate the State as a "co-party", which is entitled to receive notice from the agent if there is any change in the status of the escrow agreement between Contractor and the agent, including notice of a proposed termination or transfer. Before the Contractor can change a designated Escrow Agent, the Escrow Agent and the Contractor shall provide the State a minimum advanced notice of sixty (60) business days of the proposed change. Before the escrow may be moved or changed, the State has to be notified of the identity of the new proposed agent, and the new agent has to confirm the same terms of escrow vis-à-vis the State's interests.

15.Compliance with Other Miscellaneous Laws

To the extent that _____ and/or the State is the recipient of any federally funded monies relating to the procurement of Services or Products under the RFP and Contract, Contractor agrees to comply with all applicable federal laws, rules and regulations including but not limited to the following areas as further set forth at Chapters II and XXX of 7 CFR and 45 CFR Parts 74 and 95 relating to:

- a. Equal Employment Opportunity as set forth in federal Executive Orders 11246 and 11375 as supplemented by 41 CFR 60, and the nondiscrimination requirements of 45 CFR Parts 80, 84 and 90, and 7 CFR Parts 15, 15b and 15d.
- b. Copeland "Anti-Kickback Act" (18 USC 874 and 40 USC 276c) which provides that all contracts/subgrants greater than \$2,000 for construction or repair must have a provision requiring compliance with 18 USC 874 as supplemented by 29 CFR Part 3, which prohibit contractors or sub recipients from inducing by any means any person employed in construction, completion or repair of public work to give up any part of compensation to which they are otherwise entitled and that the recipient shall report all suspected/reported violations to the Federal awarding agency.
- c. Davis-Bacon Act, as amended (40 U.S.C. 276a to a-7) which requires all construction contracts awarded by recipients of more than \$2000 to comply with the Act as supplemented by USDOL Regulations 29 CFR Part 5 requiring all contractors to pay wages to laborers and mechanics at a rate not less than the minimum wage specified by the Federal Secretary of Labor, which wages shall be paid not less than once a week. The

recipient shall place a copy of the federally specified wage (the "prevailing wage") in each solicitation and the award of a contract shall be conditioned upon acceptance of such a determination. The recipient must report all suspected/reported violations to the Federal awarding agency.

- d. Contract Work Hours and Safety Standards Act (40 U.S.C. 327-333) which requires, where applicable, that all construction contracts and other contracts involving employment of mechanics and laborers require compliance with 40 U.S.C. 327-333 as supplemented by USDOL Regulations 29 CFR 5 when said contracts exceed \$100,000, which references require that work in excess of 40 hours/week be recompensed at a rate at least 50% greater than the basic pay rate and that no work be required in unsanitary, hazardous, or dangerous conditions. These requirements do not apply to the purchases of supplies, materials, or articles ordinarily available on the open market or contracts for transportation or transmission of intelligence.
- e. Rights to Inventions Made under a Contract or Agreement -Contracts or Agreements for the performance of experimental, developmental, or research work shall provide for the rights of the federal government and the recipient in any in any resulting invention in accordance with 37 CFR Part 401 and any further implementing regulations issued by USDHHS or USDA.
- f. Ownership Rights in Software or Modifications Thereof – The State shall have all ownership rights in software or modifications thereof and associated documentation designed, developed or installed with Federal financial participation, and the federal government reserves a royalty-free, nonexclusive, and irrevocable license to reproduce, publish, or otherwise use and to authorize others to use for Federal Government purposes, such software, modifications, and documentation, provided, however, that this sentence shall not apply to ‘proprietary operating/vendor software packages’ within the meaning of 45 CFR 95.617(c) and 7 CFR 277.18(l)(1)(iii).
- g. Clean Air Act (42 U.S.C. 7401 et seq.) and the Federal Water Pollution Control Act as amended (33 U.S.C. 1251 et seq.), which require Contracts and subgrants in excess of \$100,000 shall require the recipient to comply with the Acts recited herein and that violations must be reported to USDHHS and the appropriate Regional Office of the Federal Environmental Protection Agency.
- h. Byrd-Anti-Lobbying Amendment (31 U.S.C. 1352)- which requires that every contractor under a contract for more than \$100,000 and every tier of

contractors or subcontractors thereunder shall file certification, as required, that said contractor will not and has not used any Federal appropriated funds to pay any person or organization for influencing or attempting to influence any federal agency, member of Congress, or an employee of a member of Congress in connection with obtaining any Federal contract, grant, or award covered by such Amendment. A contractor or subcontractor from any tier shall also disclose any lobbying with non-federal funds that takes place in conjunction with obtaining a federal award, which disclosure shall be forwarded up any applicable tiers to the recipient. (See also 45 CFR 93)

i. Debarment and Suspension. (Federal E.O.s 12549 and 12689)- Certain contracts shall not be awarded to parties listed on the non-procurement portion of the U. S. General Services Administration's "Lists of Parties Excluded from Federal Procurement or Nonprocurement Programs" in accordance with E.O.s 12549 and 12689. (See 45 CFR 76.) Contractors with awards that exceed the simplified acquisition threshold shall provide the required certification regarding their exclusion status and that of their principals prior to award.

j. Contractor shall make positive efforts to assure that small businesses and minority and women owned business enterprises (M/WBEs) are utilized when possible as sources of supplies, equipment, construction and services. If any subcontracts are to be let, Contractor shall (1) include qualified small businesses and M/WBEs on solicitation lists; (2) assure that they are solicited whenever they are potential sources; (3) when economically feasible, divide total requirements into smaller tasks or quantities so as to permit maximum small business and M/WBE participation; (4) where the requirement permits, establish delivery schedules which will encourage participation by small businesses and M/WBEs, and; (5) use the services and assistance of the New York State Department of Economic Development [(518) 292-5100, or its WebSite at www.esc.ny.gov,] the U.S Small Business Administration, the Office of Minority Business Enterprise of the US Department of Commerce and the U.S. Community Services Administration, as appropriate.

k. Contractor shall ensure that the contract provisions specified in 45 CFR 74.48 are included in all subcontracts.

In addition, the State shall adhere to and the Contractor and any of its subcontractors shall abide by Chapter 22 of the Laws of 2014, the Service-Disabled Veteran-Owned Business Act, and any regulations and/or applicable directives which may be adopted or implemented.

Termination

In addition to termination provisions heretofore specified in this RFP, the following additional termination provisions shall apply

- a. The Agreement may be terminated by mutual written agreement of the Parties.
- b. This Agreement, may be terminated by _____ or the State, upon written notice if: Key Employees leave the employment of Contractor; the Contractor is adjudged bankrupt; the Contractor makes a general assignment for the benefit of creditors; a receiver is appointed due to the Contractor's insolvency; a petition in bankruptcy or insolvency is filed, by or against the Contractor; or the Contractor persistently disregards laws, ordinances, rules, regulations or orders of any public authority having jurisdiction.
- c. This Agreement may be terminated by _____ or the State for cause upon the failure of the Contractor to comply with the terms and conditions of this Agreement, provided _____ or the State gives the Contractor not less than thirty (30) calendar day's written notice and an opportunity to cure all items not in compliance with the terms and conditions of this agreement, including the attachments hereto. Termination shall be immediately effective upon receipt of such written notice. The Contractor agrees to incur no new obligations nor to claim for any expenses made after receipt of the notification of termination. Termination for cause shall create a liability upon the Contractor for legal damages.
- d. This Agreement may be terminated without cause, for convenience or as may be determined by _____ or the State to be in the best interest of the State, for reasons, including, but not limited to, changes in law or program administration and budgetary constraints. _____ or the State shall give written notice to the Contractor not less than thirty (30) calendar days prior to the date upon which termination shall become effective. Such written notice shall be provided via registered or certified mail, return receipt requested or hand-delivered to the other party. The date of such notice will be deemed to be the date of postmark in the case of mail or the date of Contractor's receipt of notice in the case of hand delivery. In the case of termination under this subsection, _____ or the State agrees to pay the Contractor for reasonable and appropriate expenses incurred in good faith. The Contractor agrees to incur no new obligations after receipt of notification of termination and to cancel as many outstanding obligations as possible.
- e. _____ or the State reserves the right to terminate this contract in the event it is found that any of the certifications filed by the Contractor

with the State of New York were intentionally false or intentionally incomplete. Upon such finding, _____ or the State may exercise its termination right by providing written notification to Contractor.

- f. If _____ or the State determines that funds are unavailable through lack of continued lawful appropriation therefore, _____ or the State shall deem the Agreement terminated immediately. _____ or the State agrees to give timely notice to the Contractor in the event of termination under this paragraph. If the initial notice is oral notification, _____ or the State shall follow this up immediately with written notice. _____ or the State will be obligated to pay the Contractor only for costs of pro rata services performed by the Contractor until such time as notice of termination is received either orally or in writing by the Contractor from _____ or the State, or for other costs of pro rata services performed as otherwise mutually agreed by both parties.
- g. In the event of termination for any reason, the Contractor shall not incur new obligations for the terminated portion and the Contractor shall cancel as many outstanding obligations as possible.
- h. Termination under any provision of this Agreement shall not relieve the Contractor of any liability to _____ or the State which it has under this Agreement, or for damages sustained by _____ or the State by reason of any breach of this Agreement. _____ may withhold any payments to the Contractor for the purpose of set-off until such time as the exact amount of damages due _____ or the State from the Contractor is determined.
- i. Termination of this Agreement, with or without cause, shall not create any liability on the part of _____ or the State for payment of any penalty, or any other liability.

General Responsibility Language

The Contractor shall at all times during the Contract term remain responsible. The Contractor agrees, if requested by the _____ of the New York State _____ or his/her designee, to

present evidence of its continuing legal authority to do business in New York State, integrity, experience, ability, prior performance, and organizational and financial capacity.

Suspension of Work (for Non-Responsibility)

The _____ of the New York State
_____ or his or her designee, in his/her sole discretion, reserves the right to suspend any or all activities under this Contract, at any time, when he/she discovers information that calls into question the responsibility of the Contractor. In the event of such suspension, the Contractor will be given written notice outlining the particulars of such suspension. Upon issuance of such notice, the Contractor must comply with the terms of the suspension order. Contract activity may resume at such time as the
_____ of the New York State
_____ or his/ her designee issues a written notice authorizing a resumption of performance under the Contract.

Termination (for Non-Responsibility)

Upon written notice to the Contractor, and a reasonable opportunity to be heard with the _____ of the New York State
_____ or staff, the Contract may be terminated by
_____ of the New York State
_____ or his/ her designee at the Contractor's expense where the Contractor is determined by the _____ of the New York State
_____ or his or her designee to be non-responsible. In such event, the _____ of the New York State
_____ or his or her designee may complete the contractual requirements in any manner he or she may deem advisable and pursue available legal or equitable remedies for breach.

In addition to the termination language related to responsibility above, the
_____ in his/her sole discretion reserves the right to terminate this Agreement, with or without cause, at any time, for convenience or as may be in the best interests of the State. Termination of the Agreement, with or without cause, shall not create any liability on the part of _____ or the State for payment of any penalty, or any other liability.

A. For Convenience

The State hereby reserves the right to terminate this Contract for convenience, or in the event that necessary and lawful appropriations are not provided or continued for the funding of this contract by the Legislature or Governor subject to and in accordance with the following provisions:

1. The State shall have the right to unilaterally terminate this Contract, in whole or in part, for convenience provided that prior notice of such termination is given. Such option may be exercised upon thirty (30) calendar days advance written notice to the Contractor pursuant to paragraph (C), below. In the event that the State exercises this option, the Contract shall terminate as to the portion(s) of work being deleted as of the termination date set forth in paragraph (C), below, with obligations of the parties as follows:

a. The Contractor shall deliver to the possession of the State within such thirty (30) calendar day notice period all drawings, reports or other required Contract deliverables to date related to the portion(s) of work subject to the termination, whether preliminary or final, in the form and format set forth in this agreement. The State's receipt of such deliverables shall be a condition precedent to the obligation of the State to make payments to the Contractor.

b. Upon receipt of such deliverables, the State shall be obligated to pay the Contractor the amounts then due and owing as specified in the Contract as the exclusive amounts due Contractor, calculated as of the termination date, such payment to be tendered to Contractor within ninety (90) business days of receipt of the deliverables. The State shall not be liable to Contractor for lost profits, administrative or other expenses, however denominated.

B. For Cause

1. Notice

If either party fails to materially comply with any provision of the Contract the other party shall so notify the party in default as provided below. The notification shall specify in reasonable detail the nature of the default.

2. Cure Period

Where timeframes for performance are otherwise set forth in this Contract, the specific time period stated shall govern. For all other instances constituting Contractor's default, the Contractor shall have thirty (30) calendar days from the date of receipt of notice to correct the default ("cure period"). During the cure period, Contractor shall work diligently to resolve and cure any default. The State may, at its discretion, agree to extend the timeframe for cure.

Because of the secure nature of the DCJS' PSCTS or any other State agencies PSCTS, the State may, upon written notice to the Contractor, shorten the aforementioned thirty (30) calendar day cure period as it deems necessary in the event that the Contractor's breach threatens or has the

Page 32 of

potential to threaten the ongoing operation of the PSCTS, or the health, safety or welfare of those served by the PSCTS.

3. Default

If the Contractor is unable to cure the default within the cure period, in addition to availing itself of specific remedies set forth in the Contract, the State may pursue all legal and equitable remedies for breach. A delay or failure in declaring a material breach under this paragraph shall not be deemed a waiver of the right to subsequently declare a default.

4. Additional State Rights & Remedies

- a. In the event of Contractor's default, in addition to pursuing any other legal or equitable remedies, the State shall have the right to take one or more of the following actions:
 - i. terminate the Contract, in whole or in part;
 - ii. proceed against any Bond or Insurance furnished by Contractor or subcontractor, in accordance with the terms thereof;
 - iii. suspend, in whole or in part, payments due Contractor under this or any other New York State Contract;
 - iv. pursue equitable remedies to compel Contractor to perform; and/or v. all rights set forth under b, below.
- b. It is expressly understood between the parties that the State is contracting with Contractor for the personal services of Contractor in building, operation and maintenance of a PSCTS and associated network which is a public safety system operated and maintained by the State for the best interests of the State and safety and welfare of the citizens of New York.

Therefore, in the event of termination of this Contract in whole or in part based upon the Contractor's default or abandonment, the State shall, in its sole judgment, among other factors, determine the usability to the State of that portion of the PSCTS completed prior to default with reference to completion of the foregoing mission. The State may, in accordance with that determination, pursue any remedies as it deems advisable in completing that mission, with sole reference to the best interests of the State, including, but not limited to:

- i. buy out all or part of the completed PSCTS or system components;
- ii. Contractor to license or grant to the State such intellectual property and patent rights for the proposed technology solution as are required for:
 - a) Continued operation and maintenance of the previously completed portion of the PSCTS, by the State or by a qualified third party selected by the State for the remainder of the original contract term, and/or;

b) the design, build, continued operation and maintenance of the uncompleted PSCTS deliverables due under the Contract;

iii. procuring from any third party, upon such terms and in such manner as the State deems appropriate, either:

a) an alternate system(s) to complete the unfinished portion of the PSCTS deliverables at time of default, and/or;

b) pursuing any other action(s) provided at law or in equity as the State deems necessary to enable the State to complete the above mission.

The Contractor shall be liable for any and all excess costs for remedies pursued by the State, and for administrative costs incurred by the State in procuring alternate services.

5. Transition

In the event that the PSCTS is operational at the point that a termination for cause is issued, the Contractor shall provide and comply with the requirements for transition set forth in the Agreement below.

6. Cumulative Remedies

The rights and remedies provided in this paragraph are cumulative to and in addition to any other rights and remedies provided by law, at equity, or under the Contract.

C. Termination Notice

Notices required by this section shall be delivered to the other party in writing, by certified mail, return receipt requested. The date of notice shall be deemed the date of delivery set forth on the return receipt. (“date of return receipt notice”) Such _____ notice shall be addressed as follows:

State of New York:

DETAIL NOTICE INFORMATION IN FINAL CONTRACT

Contractor:

D. Termination Date

Contract termination dates shall be determined as follows:

In the event a notice of termination is issued for convenience, the Contract termination date shall be deemed ninety (90) calendar days from the date of delivery set forth on the return receipt notice.

Subject to the State's right to shorten the cure period pursuant to paragraph (B), above, in the event a notice of termination is issued for cause, the Contract termination date shall be from the date of the return receipt notice, or such other extended period of time as has been mutually agreed in writing by the parties.

E. Mitigation of Costs

The Contractor shall not undertake any additional or new Contractual obligations on or after the date of return receipt notice of a termination notice without the prior written approval of the State. On or after the date of return receipt notice of a termination notice and during the termination notice period, the Contractor shall take all commercially reasonable and prudent actions to close out unnecessary outstanding, existing obligations as economically as possible for the State.

F. Asset Accounting & Transfer

Within thirty (30) calendar days of receipt of a termination notice, the Contractor shall be required to update and finalize a complete inventory of the PSCTS infrastructure, supplies, equipment and other tangible or intangible assets. ("assets") To the extent that such assets are subject to a financing or other lease agreement as of the date of notice, and that the State has exercised the purchase option as to such asset(s) or has elected to complete the PSCTS mission in accordance with this Agreement, above, the State may require Contractor to execute all necessary and appropriate legal documents evidencing a transfer of ownership or assignment of Contractor's interest in such assets to the State or other third party designated by the State as the State or Contractor's successor in interest.

Post Termination Transition

Because of the public safety interests of the State, the State may require the Contractor to provide uninterrupted services after Contract termination as the State deems reasonable and necessary for the continued safe operation of the PSCTS and/or as necessary for the State to comply with all legal requirements for establishing a new Contract to continue safe operation of the PSCTS ("transition period"). Transition services shall be governed as follows:

A. Post Termination Transition Period

The post termination transition period shall be determined by the State, and set forth in writing, return receipt notice, to the Contractor. The State shall consult with the Contractor prior to making such determination. The State reserves the right to subsequently amend the post

termination transition period upon thirty (30) calendar days advance written notice to the Contractor.

B. No Interruption in Service

At all times during the post termination transition period and unless waived by the State, the Contractor shall continue all Contractual obligations set forth in the Contract until such time as the State (i) has approved the Contractor's proposed post termination transition plan, and (ii) an orderly post termination transition to the State or a new Contractor has been completed pursuant to the approved post termination transition plan. The Contractor shall be required to meet its Contractual obligations pursuant to this paragraph notwithstanding the issuance of a termination for cause.

C. Post Termination Transition Plan

Within fifteen (15) calendar days of receipt of a notice of termination as set forth elsewhere in the Contract or twelve months prior to the end of the term of the Agreement, whichever event occurs first, the Contractor shall provide for approval by NYS a detailed written plan for Post Termination Transition (Post Termination Transition Plan) which outlines, at a minimum, the tasks, milestones and deliverables associated with the smooth transition of the PSCTS to a successor Contractor, as applicable. Furthermore, the Post Termination Transition Plan must be amended by Contractor to include all other information deemed essential by the State, including development of specifications necessary for preparation of a competitive solicitation for the successor Contract.

D. Contractor Post Termination Transition Services

"Post termination transition services" shall be deemed to include Contractor's responsibility for all tasks and services outlined in the Contract, and for transferring in a planned manner specified in the Post Termination Transition Plan all tasks and services to the State or successor Contractor. It is expressly agreed between the parties that the level of service during the post termination transition period shall be maintained in accordance with and shall be subject to all the terms and conditions of the Contract, provided, however, that where, during the post termination transition period, tasks or services are transitioned to or assumed by the State or the successor Contractor, Contractor shall not be held responsible for the acts or omissions of the State or successor Contractor or for service degradation resulting from the acts or omissions of the State or successor Contractor. The Contractor shall transfer to the successor Contractor all title, leasing rights, or license rights of all hardware and equipment in use in the PSCTS operation. The successor Contractor shall utilize such hardware and equipment in accord with the rights and duties attendant thereto. The Contractor shall turn over to the successor Contractor all network software, data files, application programs, and documentation.

E. Compensation for Post Termination Transition Services

Contractor shall be reimbursed for services performed during the post termination transition period at the rates previously set forth in the Contract.

F. State Responsibilities for Post Termination Transition

The State shall assume responsibility for post termination transition project management. A project manager responsible for coordinating post termination transition activities, maintaining the transition task schedule, and approving transition deliverables shall be appointed. Periodic project review meetings shall be held with representatives of the State, the Contractor, and the successor Contractor.

G. Training Successor Organization & Personnel

Post Termination Transition Services furnished by the Contractor must include the development of a training plan. The Contractor is required to provide post termination transition training for the successor organization's management in the operation and maintenance of the PSCTS. The training effort shall focus on providing the successor Contractor's management personnel with information about all operational aspects of the PSCTS. During transition, the Contractor shall prepare a detailed training program. This program shall establish a post termination transition training group which shall provide the required training for successor Contractor personnel.

Training shall be accomplished through a mixture of formal and on-the-job training. The successor Contractor's management personnel shall participate in all PSCTS related functions during the post termination transition period. The successor Contractor's management shall be asked to participate in normal operations and to fulfill required tasks. The Contractor agent shall also provide documented instructional materials to facilitate the learning process. The latest version of all documentation shall be used during the formal training sessions.

Rescale of Project

The State reserves the right to terminate or modify this Agreement in the event of loss or change of funding streams or appropriations. The State reserves the option to rescale the capacity and/or functionality of the PSCTS or the contractual requirements in order to serve the best interests of the State. If the State exercises the option to reduce the scope, any proposed modifications to insure the performance or interoperability of the modified network will be subject to the Change Order provisions set forth below. If the State exercises the option to scale back the project, the State shall be entitled to a corresponding adjustment in fees due the Contractor with no further compensation due Contractor for any deleted scope.

Process for Change Orders

At any time during the term of this Contract, the State may make changes, subtractions or additions in any of the Equipment, Software, Documentation, Services and/or other Deliverables within the general scope of work set forth in the Contract, consistent with pricing established

under the terms of this agreement. Such changes will be subject to the unit costs itemized in the Contract or such other costs as may be mutually agreed between the parties. All such changes shall be reduced to a written Change Order (Appendix J of the RFP) executed by both parties, and shall otherwise be in accordance with the terms and conditions of this Contract. The Change Order shall be accepted and agreed to by both the State and the Contractor as evidenced by the written signatures of the appropriate representatives of both parties. If any such change causes an increase or decrease in pricing or the time required for the performance of the Contract, an equitable adjustment of the Contract amount and/or time of performance will be made on mutual agreement of the parties, subject to the approval of the New York State Comptroller and any applicable control agency, if required.

Force Majeure

In the event of a service disruption caused by a Force Majeure which is outside of the control of either party, e.g., natural disaster, act of God, war, terrorism, civil disturbance, court order or labor dispute, ("force majeure") or any other acts beyond the reasonable control of either party, the party that has been so affected shall immediately give notice to the other party, and shall exercise every commercially reasonable effort to resume performance, and an extension of the time for performance shall be granted for a period to be agreed to in writing by the State and Contractor.

In the event of a service disruption caused by a State Disaster Emergency, as defined in Section 20(2)(b) of the Executive Law or other emergency situation or occurrence that the _____ of the _____, the Governor, or any other State agency head in his/her sole discretion, has determined poses a risk to health and public safety or the conservation of public resources, the Contractor shall be notified that DCJS or the State is invoking this provision and that notwithstanding any other provision in the Contract, during a State disaster emergency or other emergency situation, unless the Contractor's performance would be excused pursuant to the *Force Majeure* provisions of the Contract, the Contractor shall provide the necessary Services to the State on a time-is-of-the-essence basis, working on a twenty-four (24) hour a day, seven (7) day a week basis, to restore and/or recover State operations and Services that are critical to the public safety, health, and welfare of the State, to be determined at the sole discretion of the State. Except as provided in this section, all other provisions of the RFP and Contract remain in full force and effect during a state disaster emergency or other emergency situation.

Press Releases

Contractor agrees that no brochure, news/media/press release, public announcement, memorandum or other information of any kind regarding the Contract shall be disseminated in any way to the public, nor shall any presentation be given regarding the Contract without the prior written approval by the undersigned or the undersigned's designee from DCJS, _____ or any other State entity where designated and applicable, which written approval shall not be unreasonably withheld or delayed provided, however, that Contractor shall be authorized to provide copies of the Contract and answer any questions relating thereto to any

State or Federal regulators or, in connection with its financial activities, to financial institutions for any private or public offering.

Security, Information Security, Breach and Notification Act

The Contractor shall maintain the security, nondisclosure and confidentiality of all information in accordance with the following clauses in performance of its activities under the Contract. Contractor shall ensure that its personnel, agents, officers and any subcontractors are fully aware of the obligations arising under this section and shall take all commercially reasonable steps to ensure compliance. Disclosure of PSCTS information developed by the State, any Authorized PSCTS User, the Contractor or their employees, subcontractors, partners or its agents is strictly prohibited. The Contract may be terminated by the State for cause for a material breach of this section.

A. Security Procedures & Employee Dishonesty

Contractor warrants, covenants and represents that it will comply fully with all security procedures of the State in performance of the Contract. Contractor shall hold the State harmless from any loss or damage to the State resulting from the violation by the Contractor, employees, and subcontractors of such security procedures or resulting from any criminal acts committed by such, employees, and subcontractors while providing services under the Contract.

B. Information Security Breach and Notification Act

Section 208 of the State Technology Law (STL) and Section 899-aa of the General Business Law (GBL) require that State entities and persons or businesses conducting business in New York who own or license computerized data which includes private information including an individual's unencrypted personal information plus one or more of the following: social security number, driver's license number or non-driver ID, account number, credit or debit card number plus security code, access code or password which permits access to an individual's financial account, must disclose to a New York resident when their private information was, or is reasonably believed to have been, acquired by a person without valid authorization. Disclosure of breach of that private information to all individuals affected or potentially affected must occur in the most expedient time possible without unreasonable delay, after necessary measures have been taken subject to approval of _____ or such other applicable State agency to determine the scope of the breach and to restore integrity, but with delay if law enforcement determines it impedes a criminal investigation.

When notification is necessary, the State entity or person or business conducting business in New York must also notify the following New York State agencies: the Attorney General, the New York State Enterprise Security Office, Division of State Police, and the Department of State's Division of Consumer Protection. Information relative to the law and the notification process is available at: <http://www.dhses.ny.gov/ocs/breach-notification/>

State entities subject to STL§208 that experience breaches of computerized data which includes private information must file notices with the New York Attorney General; Department of State's Division of Consumer Protection; and the Office of Information Technology Services' Enterprise Information Security Office.

GBL§899-aa provides that persons or businesses conducting business in New York must disclose any breaches of computerized data which includes private information by notifying the offices of the New York Attorney General; the NYS Division of State Police; and the Department of State's Division of Consumer Protection.

Information relative to the law and the notification process is available at: <http://www.dhses.ny.gov/ocs/breach-notification/>

Indemnification of New York State and Authorized Users for Breach of Security

The Contractor will indemnify DCJS, _____ and the State *without limitation* against any claims brought against DCJS, _____ and/or the State by reason of a wrongful disclosure of confidential information attributed to the Contractor or any of its agents, employees, and/or subcontractors and will cooperate fully with DCJS, _____, the State, and the Attorney General in defense of any claim(s).

GBL§ 899-aa provides in part that:

6. (a) whenever the Attorney General shall believe from evidence satisfactory to him/her that there is a violation of this article he/she may bring an action in the name and on behalf of the people of the state of New York, in a court of justice having jurisdiction to issue an injunction, to enjoin and restrain the continuation of such violation. In such action, preliminary relief may be granted under article sixty-three of the civil practice law and rules. In such action the court may award damages for actual costs or losses incurred by a person entitled to notice pursuant to this article, if notification was not provided to such person pursuant to this article, including consequential financial losses. Whenever the court shall determine in such action that a person or business violated this article knowingly or recklessly, the court may impose a civil penalty of the greater of five thousand dollars or up to ten dollars per instance of failed notification, provided that the latter amount shall not exceed one hundred fifty thousand dollars.

The remedies in GBL§899-aa(6)(a) are in addition to any other lawful remedy and in addition to any other remedy available under the terms of the Contract executed between the State and the Contractor.

The Contract executed between the State and the Contractor may be terminated by the State for cause for a material breach of this section, and the provisions of GBL§ 899-aa shall survive the termination of this Agreement.

Nondisclosure & Confidentiality

The following shall supplement the requirements of Appendix B, General Specifications, paragraph 14 and subsection 5.14.(D) of the RFP. Except as may be required by applicable law or a court of competent jurisdiction, the Contractor, its officers, agents, employees, and subcontractors, if any, shall maintain strict confidence with respect to any Confidential Information to which the Contractor, its officers, agents, employees, and subcontractors, if any, have access. The terms of this Section shall survive termination or expiration of this Contract. Contractor agrees that its officers, agents, employees, and subcontractors, if any, performing Services for the State under this Contract shall be made aware of and shall agree in writing to the terms of this Section. For purposes of this Contract, all State or Authorized Users information of which Contractor, its officers, agents, employees, and subcontractors, if any, becomes aware during the course of performing Services for the State shall be deemed to be confidential Information (oral, visual or written).

All information will be accounted for by the Contractor upon receipt and properly stored before, during, and after processing. In addition, all related output will be given the same level of protection as required for the source material.

The Contractor agrees that the data processed during the performance of the Contract will be completely purged from all data storage components of the Contractor's computer facility and no output will be retained by the Contractor at the time the work is completed, except for the documents required to be maintained pursuant to Section 5.7 of the RFP and Appendix A paragraph 10. If immediate purging of all data storage components is not possible, the Contractor will certify that any data remaining in any storage component will be safeguarded to prevent unauthorized disclosures.

The Contractor will be responsible for the destruction of any intermediate hard copy printouts and will provide the _____ Project Manager, his/her designee, or any other named State employee or his/her designee with a statement containing the date of the destruction, description of material destroyed, and the method used. In the event that it becomes necessary for the Contractor to receive confidential information, which Federal or State statute or regulation prohibits from disclosure, the Contractor hereby agrees to return or destroy all such confidential information that has been received from the State when the purpose that necessitated its receipt by the Contractor has been completed. In addition, Contractor agrees not to retain any confidential information which Federal or State statute or regulation prohibits from disclosure after termination of the Contract.

Notwithstanding the foregoing, if the return or destruction of the confidential information is not feasible, the Contractor agrees to extend the protections of the Contract for as long as necessary to protect the confidential information and to limit any further use or disclosure of that confidential information by the Contractor. If Contractor elects to destroy confidential information, it shall use reasonable efforts to achieve the same and notify the State accordingly. The Contractor agrees that it will use all appropriate safeguards to prevent any unauthorized use or unauthorized disclosure of the State's confidential information, which Federal or State statute or regulation prohibits from disclosure.

The Contractor shall never disclose information which Federal, State statute, or regulation prohibits from disclosure.

The Contractor agrees that it shall immediately report to the State the discovery of any unauthorized use or unauthorized disclosure of such confidential information of any New York State agency or other Authorized User information directly to that New York State agency or other Authorized User.

Contractor shall hold the State harmless from any loss or damage to the State resulting from the disclosure by the Contractor, its officers, agents, employees, and subcontractors of such Confidential Information.

The State will have the right to terminate the Contract for cause if the Contractor fails to provide the safeguards described above or it is determined that the Contractor has violated a material term of this Section.

Notwithstanding the language contained in this Section, the Contractor may release any information pursuant to a final order issued from a Court of competent jurisdiction, provided the State has had an opportunity to be heard by such Court.

Notwithstanding the foregoing, information which falls into any of the following categories shall not be considered confidential information:

- a. Information that is previously rightfully known to the receiving party and accessible without restriction on disclosure;
- b. Information that becomes, from no act or failure to act on the part of the receiving party, generally known in the relevant industry or is in the public domain;
- c. Information that is independently developed by the Contractor without use of confidential information of the State;
- d. Information unrelated to the scope of this engagement; and
- e. That the State has approved for disclosure, but solely in accordance with the State's approval or direction.

Security

The following shall supplement the requirements of Appendix B paragraph 69 of the RFP. Contractor warrants, covenants and represents that it shall comply fully with all security procedures and policies of the State during the performance of the Contract. Contractor shall hold the State harmless from any loss or damage to the State resulting from the violation by the Contractor, its officers, agents, employees, and subcontractors, if any of such security procedures or policies resulting from any criminal acts committed by such officers, agents, employees, and subcontractors, while providing Services under the Contract.

The specific security procedures the Contractor shall implement include, but are not limited to:

A. Data Access and Location– the Contractor must ensure that all data related to this project is stored in a controlled access environment to ensure data security and integrity. All access to State data, physical or virtual, must be conducted within the Continental United States and have adequate security systems in place to protect against the unauthorized access to the facilities and data stored therein. Adequate security systems must be in place to control access into the facilities. The Contractor shall not send or permit to be sent to any location outside of the Continental United States any data related to this project. Access into and within the facilities must be restricted through an access control system that requires positive identification of authorized individuals as well as maintains a log of all accesses (e.g., date, time, who). The Contractor shall have a formal procedure in place for granting computer system access to the data and to track access. Access for projects outside of those approved by the State or an Authorized User is prohibited.

B. Data Transport – The Contractor shall use reputable means to transport data. Deliveries must be made either via hand delivery by an employee of the Contractor or by restricted delivery via courier (e.g., FedEx, United Parcel Service, United States Postal Service) with shipment tracking and receipt confirmation. This applies to transport between the Contractor’s offices, to and from subcontractors, and to the State.

C. Data Protection – The Contractor shall use appropriate means to preserve and protect data related to this project. This includes, but is not limited to, use of stable storage media, regular data backups and archiving, password protection of volumes, and data encryption. The Contractor shall encrypt data identified by the State and using encryption methods approved by the State.

D. Data Wiping – At the termination of the Contract, the Contractor will be required to wipe all data storage devices to eliminate any and all State data either collected or generated by the Contractor or provided by the State except for the documents required to be maintained pursuant to Appendix A paragraph 10. The wiping process must meet requirements set by the State.

E. Data Breach Notification –Contractor agrees that it shall immediately report to the State the discovery of any unauthorized use or unauthorized disclosure of such Confidential Information of any New York State agency information directly to that New York State agency.

G. Security Audits - Contractors may be asked to provide a recent independent audit report on security controls prior to formal awarding of any contract resulting from this RFP or at any time during the Contract term. The State and any regulatory authority having jurisdiction over the State or Authorized Users shall have the right to send its officers and employees into the offices and plants of the Contractor for inspection of the facilities and operations used in the performance of any work under the resulting Contract. On the basis of such inspection, specific measures may be required in cases where the Contractor is found to be noncompliant with Contract safeguards.

Criminal Justice Information Services (CJIS)

This RFP and its resulting Contract are strictly limited to permitting the Contractor to perform the services as described in the RFP and its resulting Contract. At no time shall the Contractor have access to any criminal history record information or other sensitive criminal justice information, including employment records contained on Authorized Users Systems or media without complying with this Section. Any access to computer media/systems which contain criminal history record information and other sensitive criminal justice information is subject to the Federal Bureau of Investigation Criminal Justice Information Services (CJIS) Security Policy, specifically the Security Addendum (SA) (annexed as Appendix D in the RFP). The purpose of the SA is to provide adequate security for criminal justice systems and information while under the management or control of a private entity or contractor. The SA strictly limits the authorized access to criminal history record information, limits the use of the information to the specific purposes for which it is being provided, ensures the security and confidentiality of the information consistent with applicable laws and regulations, provides for sanctions, and contains such other provisions as required by the FBI Director. Upon selection, the selected bidder and as a condition precedent for providing Project Services for the benefit of the Authorized Users, and as evidenced by the Successful Bidder signing the Contract, the Successful Bidder agrees (1) to abide by the SA, and (2) to the incorporation by reference of the SA as a part of the Contract, (3) that the SA shall be incorporated by reference as a part of all subcontract entered into by the Successful Bidder the purpose of which is of the delivery of Project Services, if any; and (4) that those Successful Bidder employees and subcontractor employees, if any that provide Project Services shall sign the form entitled, "Federal Bureau of Investigation Criminal Justice Information Services Security Addendum Certification" as set forth in RFP, Attachment 22. One copy of the signed form will be retained by the Successful Bidder and the original will be provided to the State for retention by the CJIS Information Security Officer for New York State.

NYS Cyber Security Policy P03-002

A. All information concerning _____'s and such other State agency's operations, procedures and policies shall be kept confidential by the Contractor and the Contractor shall comply with administrative procedures and regulations concerning these rules. The Contractor shall take all steps required by _____ or the State to protect confidential information. This will include fingerprint and background checks of Contractor personnel or any Contractor's approved Subcontractor with access to such information and a requirement that the Contractor replace personnel or any such Subcontractor at the discretion of _____ or the State.

B. Contractor must abide by the conditions set forth in Appendix O of the RFP, Cyber-Security-Policy-P03-002-V3.4 c. As a result of the security issues associated with the services to be performed by the Contractor, the Contractor and any associates and/or Subcontractors will be required to insure that all work is performed within the continental United States.

User Data is the Property of New York State

In the course of performance of its obligations pursuant to this RFP and any resulting Contract the Contractor, its personnel, agents, officers, and any Subcontractors may have access to or

come into possession of data and information which is the property of _____ or the State and data and information which is processed by or stored within _____ or another State agency for the benefit of itself or other entities. Such data includes but is not limited to employee and license application information, social security numbers, personally identifying information, photographs, and other data and information stored in electronic, optical or physical form including data and information concerning individuals and data and information concerning operations, processes, procedures and policies of _____ and other governmental entities.

All information concerning such aforementioned State operations, procedures and policies shall be kept confidential by the Contractor, its personnel, agents, officers, and any Subcontractors, and the Contractor shall ensure that it and any such individuals or entities comply with _____ and/or other State Agency administrative policies/procedures, regulations or requirements and take all steps required by _____ and any other State agency to protect confidential information. This may include, but is not limited to, execution of non-disclosure agreements by Contractor's or Subcontractor's personnel, agents, officers, and employees. If applicable to the environment, fingerprint checks and New York State Police background checks of the Contractor's personnel, agents, officers, or employees and the employees of any Subcontractors with access to such information in connection with the project, and a requirement that any Contractor's personnel, agents, and officers and the employees of any Subcontractor must be approved by _____. The Contractor shall be responsible for assuring the State that it has notified all such individuals involved with the contract of the provisions of this Section, and the Contractor shall require compliance with the provisions of this section by performing or providing necessary in connection with this RFP and the resulting Contract.

The use of information obtained by such aforementioned Contractor and/or Subcontractor individuals in the performance of its duties under this Agreement shall be limited to purposes directly connected with such duties with the understanding that none acquire any ownership, right to use, title or any interest in any data or information which remains the property of _____ or the State or the property of the entities for which _____ or the State is processing or storing the data or information.

The Contractor shall take appropriate precautions to ensure that Contractor's personnel, agents, and officers and the employees of any of its subcontractors;(i) shall never remove any work papers or product from _____ or any other State premises except with the written consent of _____ or another designated State agency and(ii) never disclose, sell, publish, archive, make available in any form or summary any information of any kind obtained in connection with performance under this RFP and any resulting Contract. The provisions of this section shall survive the termination of this Agreement.

Accounting/Audit

A. Maintenance of Supporting Documentation

The Contractor shall maintain all documentation supporting costs charged to the project, which shall be maintained for a minimum of seven (7) years beyond the Contract termination or any Contract amendment termination date.

B. Access to & Audit of Agreement Records

At all times during the contractual term and for a period of seven (7) years thereafter, the Contractor shall provide the NYS Comptroller, the Attorney General, and any other person or entity authorized to conduct an examination, as well as any other agencies or entities involved in this contract, with full access to the supporting documentation that pertains to services performed and determination of amounts payable under the Contract. Access shall be granted within five (5) business days. The Contractor will also make the appropriate individuals with knowledge of the supporting documentation of financial records related to the Contract (including the Contractor's independent public auditors) available to State representatives to answer questions and provide additional documentation where necessary. State representatives shall be permitted to examine, audit and copy such records at the site at which they are located. The Contractor shall be responsible for assuring that the provisions of this Section shall apply to any subcontract related to performance under the Contract.

Minority & Women Owned Business Enterprises

NEW YORK STATE LAW

Pursuant to New York State Executive Law Article 15-A, DCJS recognizes its obligation under the law to promote opportunities for maximum feasible participation of certified minority-and women-owned business enterprises and the employment of minority group members and women in the performance of DCJS contracts.

In 2006, the State of New York commissioned a disparity study to evaluate whether minority and women-owned business enterprises had a full and fair opportunity to participate in state contracting. The findings of the study were published on April 29, 2010, under the title "The State of Minority and Women-Owned Business Enterprises: Evidence from New York" ("Disparity Study"). The report found evidence of statistically significant disparities between the level of participation of minority-and women-owned business enterprises in state procurement contracting versus the number of minority-and women-owned business enterprises that were ready, willing and able to participate in state procurements. As a result of these findings, the Disparity Study made recommendations concerning the implementation and operation of the statewide certified minority- and women-owned business enterprises program. The recommendations from the Disparity Study culminated in the enactment and the implementation of New York State Executive Law Article 15-A, which requires, among other things, that DCJS establishes goals for maximum feasible participation of New York State Certified minority- and women – owned business enterprises ("MWBE") and the employment of minority groups members and women in the performance of New York State contracts.

Business Participation Opportunities for MWBEs

For purposes of this Contract, the State hereby establishes an overall goal of 20% for MWBE participation, 15% for Minority-Owned Business Enterprises (“MBE”) participation and 5% for Women-Owned Business Enterprises (“WBE”) participation (based on the current availability of qualified MBEs and WBEs). The Contractor shall attempt to utilize, in “good faith”, any MBE or WBE identified within its MWBE Utilization Plan, during the performance of the Contract. The Contractor must document “good faith” efforts to provide meaningful participation by MWBEs as subcontractors or suppliers in the performance of the Contract and Contractor agrees that _____ may withhold payment pending receipt of the required MWBE documentation. The directory of New York State Certified MWBEs is available at <http://www.nylovesmwbe.ny.gov>.

Requests for a partial or total waiver of established goal requirements made subsequent to Contract execution may be made at any time during the term of the Contract to _____ but must be made no later than prior to the submission of a request for final payment on the Contract.

For guidance on how _____ will determine a Contractor’s “good faith efforts,” the Contractor agrees to review the provisions of 5 NYCRR §142.8.

In order to document the progress made toward achievement of the MWBE goals of the Contract, Contractor must agree to complete and submit the following forms in compliance with the instructions contained within each form or as _____ may otherwise advise and Contractor so agrees:

MWBE Subcontractor Utilization Quarterly Report

This form must be completed and submitted to _____ each quarter throughout the term of this Contract. Contractor is required to report the actual payments made to all certified minority or women owned businesses not later than the 10th calendar day following the end of each quarter over the term of the Contract. Forms and instructions are available in Appendix C of this Contract.

Work Force Employment Utilization Report

This form must be completed and submitted to _____ each quarter throughout the term of this Contract. Contractor is required to report the actual work force utilized in the performance of the Contract broken down by specified categories. Forms and instructions are available in Appendix C of this Contract.

MWBE Request for Waiver Form

This form may be submitted by the Contractor if it has taken every “good faith effort” to promote MWBE participation pursuant to the MWBE requirements as set forth under the Contract, but has not succeeded in reaching the contractual MWBE goals. Forms and instructions are available in Appendix C of this Contract.

Should _____ determine that the Contractor has willfully and intentionally failed to comply with the minority and women-owned participation requirements of Executive Law Article 15-A, the Contractor shall be liable to the State for liquidated or other appropriate damages and the State may pursue appropriate remedies on account of such breach, including withholding payment from the Contractor.

Such liquidated damages shall be calculated as an amount equaling the difference between: (1) all sums identified for payment to MWBEs had the Contractor achieved the contractual MWBE goals; and (2) all sums actually paid to MWBEs for work performed or materials supplied under the Contract.

Equal Employment Opportunity Requirements

The Contractor agrees with all of the terms and conditions of Appendix A including Clause 12 - Equal Employment Opportunities for Minorities and Women. The Contractor is required to ensure that it and any subcontractors awarded a subcontract over \$25,000 for the construction, demolition, replacement, major repair, renovation, planning or design of real property and improvements thereon (the "Work") except where the Work is for the beneficial use of the Contractor, shall undertake or continue programs to ensure that minority group members and women are afforded equal employment opportunities without discrimination because of race, creed, color, national origin, sex, age, disability or marital status. For these purposes, equal opportunity shall apply in the areas of recruitment, employment, job assignment, promotion, upgrading, demotion, transfer, layoff, termination, and rates of pay or other forms of compensation. This requirement does not apply to: (i) work, goods, or services unrelated to the Contract; or (ii) employment outside New York State.

Further, pursuant to Article 15 of the Executive Law (the “Human Rights Law”), all other State and Federal statutory and constitutional non-discrimination provisions, the Contractor and subcontractors will not discriminate against any employee or applicant for employment because of race, creed (religion), color, sex, national origin, sexual orientation, military status, age, disability, predisposing genetic characteristic, marital status or domestic violence victim status, and shall also follow the requirements of the Human Rights Law with regard to non-discrimination on the basis of prior criminal conviction and prior arrest.

Failure to comply with any the foregoing MWBE or Equal Employment requirements may result in a finding of non-responsibility and/or a breach of the Contract, leading to the withholding of funds, suspension or termination of the Contract or such other actions or enforcement proceedings as allowed by the Contract.

Payment of Outstanding Tax Liabilities

All outstanding tax liabilities if any, against the Contractor in favor of the State of New York must be satisfied prior to Contract execution or a payment schedule acceptable to the State of New York arranged for their speedy satisfaction.

Dispute Resolution and Escalation

In addition to any escalation procedure or problem resolution procedure established in connection with the delivery of specific Deliverables or Services under this Agreement, the State and the Contractor shall have recourse to the dispute resolution procedure described herein. State staff and Contractor staff shall, in good faith and in a timely manner; attempt to resolve all disputes arising under this Agreement. The State and the Contractor agree to the use of the following procedures should a dispute arise concerning their rights and responsibilities under this Agreement:

A. The State's Project Manager and Contractor's Project Manager will be given the first opportunity to solve the dispute.

B. If the Project Managers cannot resolve the dispute within five (5) business days from the date on which the dispute arose, they will refer the dispute, in writing, to the ITS Public Safety Cluster CIO or designee and the Contractor's signatory or designee. The memo will contain a description of the disputed issue and the date of event causing the dispute.

C. Contractor shall, in conjunction with the reporting requirements set forth herein, provide the State with a written report quarterly of those disputes requiring action under paragraph B, above. Such report shall include an explanation of how each such dispute was resolved.

D. The foregoing dispute resolution procedure, or any determination or equitable allocation of costs included therein, shall not be deemed to limit either Party's rights or remedies under this Agreement.

E. Another State agency procuring Contractor PSCTS services may establish another dispute resolution procedure to follow, however must provide written notice in advance to the Contractor.

Additional Responsibilities of the Contractor

- a. If the Contractor's proposal includes goods or services provided by another firm, the Contractor shall assume full responsibility for the delivery, installation, maintenance and support services of such items offered in the proposal. The State will contract only with the Contractor. The State shall consider the Contractor to be the sole contact with regard to all provisions of the Contract.
- b. The Contractor is responsible for meeting all obligations set forth in this RFP and any resulting Contract, including all exhibits, appendices and addenda, and any subsequent amendments mutually agreed to in writing between the parties. The Contractor acknowledges that the Contract is being entered into by the State in reliance on Contractor's representations concerning the particular qualifications, expertise, experience, financial standing and resources, management expertise and technical expertise of the Contractor and its staff assigned to provide Services under the Contract.
- c. Throughout the Contract term, in addition to the requirements of the State Finance Law § 138 (requiring the State's approval of Subcontractors), in the event that there is a substantial or material change, as defined below, in the ownership or financial viability of the Contractor, its corporate affiliates, subsidiaries, or divisions, the Contractor is required to provide notice and details of any such change to the State in writing immediately when such is first known by Contractor, its corporate affiliates, subsidiaries or divisions, or subcontractors. "Substantial" or "material" change shall be defined to include, but not be limited to; sale, acquisitions, mergers, or takeovers involving the Contractor, its corporate affiliates, subsidiaries or divisions, or partners that result in a change in the controlling ownership or assets of such entity after the submission of the Proposal; or entry of an order for relief under Title 11 of the United States Code; the making of a general assignment for the benefit of creditors; the appointment of a general receiver or trustee in bankruptcy of Contractor's, its corporate affiliates, subsidiaries or divisions, or partners' business or property; or action by Contractor, its corporate affiliates, subsidiaries or divisions, or partners under any state insolvency or similar law for the purposes of its bankruptcy, reorganization or liquidation; or court ordered liquidation against Contractor, its corporate affiliates, subsidiaries or divisions, or partners. Upon the State's receipt of such notice, the State shall have thirty (30) business days from the date of notice to review the information. The Contractor may not transfer the Contract among corporate affiliates, subsidiaries or divisions, or partners without the written consent of the State. In addition to any other remedies available at law or equity, the State shall have the right to prospectively cancel the Contract, in whole or in part, for cause if it finds that such change materially and adversely affects the delivery of Services solely determined with reference to the best interests of the State.
- d. The Contractor shall acquire the prior written approval of the State before it assigns its right to receive payment under the Contract.
- e. The Contractor shall notify the State in writing of any changes in the person or persons authorized to sign amendments to the Contract on behalf of the Contractor.

f. The Contractor shall assume sole and complete responsibility for the cost and timely completion of all activities required under this RFP and any resulting Contract.

g. The Contractor shall fully cooperate with any other contractors, such as hardware providers, that may be engaged by the State or User to work on the project.

h. The Contractor shall disclose the names and addresses of those subcontractors whose products or services materially contribute to the product or service procured from the Contractor (see Attachments 18 and 19 of the RFP). The Contractor must guarantee the work of subcontractors as if it were its own.

i. Provide a full-time Project Manager dedicated to the PSCTS project. The Project Manager must be fluent in the English language (e.g., listens, speaks, reads, writes, understands, and comprehends English fluently). This manager will be responsible for directing the work of the Contractor resources, coordinating and communicating with the DCJS Project Manager and ensuring the project deliverables are met according to the Project Plan.

j. Provide an Account Manager dedicated to the _____ account. The Account Manager must be fluent in the English language (e.g., listens, speaks, reads, writes, understands, and comprehends English fluently). This manager, separate from the Project Manager, will be responsible for directly interfacing with the Stakeholders of the PSCTS project.

k. Maintain the continuity of the Contractor team staffing throughout the course of the implementation phase of the project. _____ reserves the right to approve/disapprove changes in Contractor resources. Replacement resources must have comparable or better skills.

l. All documentation offered to the Contractor firms to assist in their efforts will be turned over to the _____ when their work has been completed. Any documentation created as part of any assignment is the property of _____ and will be turned over to _____ in paper and/or electronic format at the discretion of _____.

New York State Responsibilities

Initially, _____ will assign a resource to act as the liaison for the agency and as a primary contact for the Contractor. The _____ contact will answer all technical and analytical questions for the Contractor in conjunction with DCJS's assigned contact person. Subsequently, another authorized State agency may assign a designated person for such purposes. Thereafter, _____ will assign a resource, as applicable.

Extension of Existing Product Line – New Products

a. Until the date of acceptance testing, if technological improvements have been made to the products available for purchase under this Contract, the Contractor may propose new products that are an extension of an existing product line or the “next generation” of an existing product line that meet or exceed the specification(s) of existing products under this Contract, if the price for the new product does not exceed:

- i. The ceiling price for the product originally offered in the Contractor’s proposal;
- ii. The current published list price of the replacement product, less any applicable Government discount; or
- iii. The price at which the replacement product is generally available for purchase, whichever is lowest.

b. The proposed new product may be subject to benchmark evaluation and all costs associated with the benchmark evaluation (e.g., transportation, benchmark fee, etc.) shall be at the Contractor’s expense.

c. Whether or not to accept or reject a proposed new product is entirely within the discretion of _____ or another authorized State agency. If the State does not accept a proposed new product, the Contractor shall continue to be obligated to deliver the original product.

- f. If accepted, the addition of the new product will be documented for the administrative purposes of _____ or such other authorized State agency by a contract amendment, by adding the new product to this Contract.

Partial Invalidity

In the event that any provision of a resulting Contract is declared or found to be illegal, unenforceable, ineffective or void, then each party shall be relieved of any obligation arising from such provision. The balance of the Contract shall remain in full force and effect, if capable of performance.

Not Employees of the State

The State and the Contractor agree that the Contractor and any Subcontractor is an independent contractor, and the Contractor and Subcontractor, its agents, officers and employees, in the performance of this Agreement, shall act in an independent capacity and not as officers or employees of the State.

Waiver

No term or provision of the Agreement shall be deemed waived and no breach excused, unless such waiver or consent shall be in writing and signed by the Party claimed to have waived or consented. No consent by a Party to, or waiver of, a breach under the Agreement shall constitute

consent to, a waiver of, or excuse for any other, different or subsequent breach. The rights, duties and remedies set forth in the Agreement shall be in addition to, and not in limitation of, rights and obligations otherwise available at law or equity.

Taxes

Except as otherwise provided by applicable Federal and State law and regulations, the State shall not be liable for the payment of any taxes under the Contract, however they are designated, levied, or imposed. Purchases made by the State are exempt from New York State local sales and use taxes and, with certain exceptions, from Federal excise taxes. To satisfy the requirements of the New York State Sales and Use Tax Law, invoices issued by the Contractor pursuant to the Contract shall reference the Contract in order to be considered sufficient evidence that the sale by Contractor was made to the State. The State is an exempt organization under Section 1116(a)(1) of the Tax Law. However, no person, firm, or corporation is exempt from paying the State Truck Mileage and Unemployment Insurance taxes and other Federal, State and local taxes to which Contractor is subject. The New York State Registration Number for the purpose of tax free transactions under the Internal Revenue Code shall be provided to the Contractor by _____. Nothing in this section shall be construed to limit the obligation of the State to reimburse Contractor for approved expenses, including valid State and local taxes, under the Contract. Sales tax registration and certification requirements must be met and documentation must be provided to _____ or any other contracting State agency by the Contractor.

Severability

In the event that one or more of the provisions of the Contract shall for any reason be declared unenforceable by a court of competent jurisdiction under the laws or regulations in force, such provision(s) shall have no effect on the validity of the remainder of the Contract, which shall then be construed as if such unenforceable provision was never contained in the Contract.

Assignment of Claim

Contractor hereby assigns to the State any and all of its claims for overcharges associated with the Contract that may arise under the antitrust laws of the United States, 15 U.S.C. Section 1, *et seq.* and the antitrust laws of the State of New York, General Business Law Section 340, *et seq.*

Notification

Any notice required by or pertaining to this Contract shall be delivered to the other Party in writing, by certified mail, return receipt requested, addressed to (unless otherwise specified in the Contract) the recipient Party's signatory to the Contract or his/her designee. The date of notice shall be deemed the date of delivery set forth on the return receipt (the "date of return receipt notice"). Such notice to _____ shall be addressed as follows:

CONTACT INFORMATION WILL BE IN FINAL CONTRACT
With a copy to:

CONTACT INFORMATION WILL BE IN FINAL CONTRACT **Contractor:**

INSERT NAME, TITLE, AND BUSINESS ADDRESS

Notice to State

The Contractor shall immediately notify any contracting State agency upon learning of any situation that can reasonably be expected to adversely affect the delivery of Services under the Contract. If such notification is verbal, the Contractor shall submit to the State a written description of the situation and a recommendation for its resolution within seven (7) business days of learning of the situation.

Work Outside the Scope of the Contract

The Contractor shall refrain from performing work outside the scope of the Contract unless such work is authorized by a properly executed written amendment to the Contract approved by the Comptroller.

Suspension of Work

_____/State reserves the right to suspend any or all activities under the Contract, at any time, in the best interests of _____ and/or the State. In the event of such suspension, the Contractor will be given a formal written notice outlining the particulars of such suspension. Examples of the reason for such suspension include, but are not limited to, a budget freeze on State spending, declaration of emergency, or other such circumstances. Upon issuance of such notice, the Contractor shall comply with the suspension order. Activity may resume at such time as _____ or the State issues a formal written notice authorizing a resumption of work.

General Provision as to Remedies

The parties may exercise their respective rights and remedies at any time, in any order, to any extent, and as often as deemed advisable, without regard to whether the exercise of one right or remedy precedes, concurs with or succeeds the exercise of another. A single or partial exercise of a remedy shall not preclude a further exercise of the right or remedy or the exercise of another right or remedy from time to time. No delay or omission in exercising a right or remedy, or delay, inaction, or waiver of any event of default, shall exhaust or impair the right or remedy or constitute a waiver of, or acquiescence to, an event otherwise constituting a breach or default under this Contract.

In addition to any other remedies available to _____ or the State under the Contract, additional remedies may include, but are not limited to, the following:

A. The right for _____ or the State to withhold payment of some or all of the amounts due and owed under the Contract until Contractor's performance is brought within the specified parameters.

B. The application of credits against amounts due and owed by _____ or the State under the Contract.

Liquidated Damages

The existing PSCTS in operation at DCJS has reached the end of its useful life. The existing system serves the PSCTS processing, database and search requirements of DCJS and law enforcement agencies throughout New York State. The new DCJS' PSCTS, which will enhance PSCTS information and incorporate existing PSCTS' database, will advance both public safety and programmatic accountability. Its failure or degradation will result in damages that are impossible to calculate. Damages include but are not limited to exposure of personal identifying information, loss of statutorily mandated retention records, loss of information of an evidentiary nature and the possible exposure of individuals in sensitive and/or undercover positions which could put said individuals in imminent danger.

Because the current system has reached the end of its useful life, DCJS and _____ is making provision for its replacement through this procurement and must ensure that the replacement PSCTS is timely completed, performs as specified, that the database conversion is executed with the required degree of accuracy and that the transition between the legacy system and the PSCTS replacement occurs on time and without incident. Similar circumstances may apply to future projects under this Agreement.

Contractor's failure to deliver or install individual project deliverables within time frames agreed to by the parties or providing timely but unacceptable deliveries may cause incalculable damage to the State and to the citizens which will be impacted by such failure.

The Contractor must agree that in the event that it fails to deliver and install the PSCTS and complete acceptance testing by the date as specified in the contract or any amendment thereof the contract shall subject Contractor to liquidated damages as determined by the State which may be in the amount of one (1.00%) percent of the contract value of any late deliverable for each day that receipt is delayed over the stated time frame, up to the full amount of the contracted price of the PSCTS.

These liquidated damages are not a penalty, but shall be in lieu of certain other remedies and may be deducted from payments due or to become due and may be assessed against the Contractor's bond or insurance, where applicable. However, notwithstanding a determination to assess liquidated damages, the State may elect to determine that the Contractor is in substantial breach of the contract and terminate the contract completely, and elect to sue for all damages

which the State has incurred; in such case the Contractor shall receive a credit for any liquidated damages it shall have paid prior to termination.

In the event that the Contractor has failed to deliver and install the PSCTS and complete acceptance testing by six months following the date on which the Comptroller approves the contract, the State shall give the Contractor written notice of the intent to assess such damages and thirty (30) calendar days opportunity to cure before the liquidated amount will be assessed against the Contractor.

This provision shall not apply to the extent or for any periods where the State or a force majeure is the cause of such delay.

Extension of Use

Any contract resulting from this RFP solicitation shall contain a provision that grants the option to allow additional State or governmental agencies to purchase from the Contractor under the terms and conditions of the contract. Political subdivisions and other authorized entities within each participating State or governmental jurisdiction may also participate in any resultant contract if such State normally allows participation by such entities. New York State reserves the right to negotiate additional discounts based on any increased volume generated by such extensions.

Foreign Nationals

The Federal Immigration Reform and Control Act, as amended, (8 USC section 1324a et al) obligates employers, such as the Contractors, to verify that all its employees are legally entitled to work in the United States. In order to verify that an individual is not an unauthorized alien, _____ reserves the right to request help from the Contractor as to Contractor documentation attesting to the legal entitlement to work in the United States for each individual assigned work under this Contract. In accordance with such law, _____ and its Authorized Users do not discriminate against individuals on the basis of national origin or citizenship.

Headings Have No Legal Significance

Headings, the Table of Contents and the Glossary included within this RFP and/or Contract, as applicable, have no legal or factual significance, and are provided for the convenience of the Contractor and may not be otherwise relied on.

Penalties for Non Performance

The aforementioned RFP sets forth the State's mandatory base system requirements for availability of the solution which the Contractor is required to meet throughout the term of the Contract and applicable extensions. Failure to meet the requirements may result in penalties for non-performance in addition to any other available remedy available to the State under the terms of this RFP and resulting Contract. As the Contractor in its RFP response has proposed a solution that meets the public safety requirements of the State and because the system is a public safety system which serves law enforcement, its failure or degradation may result in damages that are impossible to calculate. Additional pecuniary damages may result from the State securing or attempting to secure replacement services for the period in which the Contractor fails to perform, although such alternatives are not capable of providing adequate cover and cannot completely mitigate the risk associated with the Contractor's failure to perform. Similar circumstances will apply to future projects under this Contract.

Reservation of Intellectual Property and Other Rights and Restrictions

- a. The State shall have all ownership rights in software or modifications thereof and associated documentation designed, developed or installed with Federal financial participation, and the federal government reserves a royalty-free, nonexclusive, and irrevocable license to reproduce, publish, or otherwise use and to authorize others to use for Federal Government purposes, such software, modifications, and documentation, provided, however, that this sentence shall not apply to 'proprietary operating/vendor software packages' within the meaning of 45 CFR 95 §617(c) and 7 CFR 277.18(l)(l)(iii). Contractor and _____ acknowledge that Contractor's Products now existing or hereafter created by Contractor are vendor software packages within the meaning of 45 CFR 95 §617(c) and 7 CFR 277 §18(1)(1)(iii). All intellectual property rights in and to Contractor's Products, including any modifications thereto, are reserved to Contractor except as provided for herein or in any SOW, Amendment or Addenda subsequently executed by the parties. All rights to use Contractor's Products are subject to separate license which shall govern the rights to use such Products. Notwithstanding the above, the modifications performed by Contractor to Contractor's Products paid for by _____ under this Agreement shall not be resold by Contractor to _____, or any other agency, instrumentality, political subdivision or municipality of the State of New York. _____ or any other agency, instrumentality, political subdivision or municipality of the State of New York shall have a royalty- free, nonexclusive, and irrevocable license to use and to authorize others to use for government purposes within New York State such modification. For clarity, the royalty-free right to use applies to modifications to Contractor's Products and not to Contractor's Products themselves, unless the parties specifically agree otherwise in a SOW or related work order. The prohibition against resale shall not restrict Contractor's right to sell services to New York State or any other agency, instrumentality or municipality of the State of New York for localization, interfacing, migration of data, installation, maintenance or further modifications of any modification or software. Finally, _____ and Contractor may agree in any SOW or related work order that certain services performed by Contractor are "work for hire." In such

case, _____ shall own such work exclusively and Contractor shall retain no intellectual property rights thereto.

Additional Miscellaneous Requirements

- a. . The Contractor agrees that its employees assigned to this Agreement will timely read the Code of Ethics of the Public Officers Law of the State of New York, set forth in sections 73 and 74, and agree not to importune any violations of those sections and the Contractor will ensure that any Subcontractor and their employees involved with this Agreement will similarly read and adhere to such provisions. Further the Contractor certifies that no individuals directly employed by Contractor who will be performing work under this Agreement are covered by §73(4)(a) which states in pertinent part that compensation greater than \$25.00 can only be made to a New York State officer or New York State employee if there was a competitive bid and public notice. Please advise if you require further information regarding this provision of law.
- b. All legal proceedings and actions brought against DCJS, _____, or the State by Contractor shall be pursued in a New York State Court of Competent Jurisdiction, and venue shall be in Albany, New York.
- c. Failure to Materially Comply

In the event of a dispute based upon an allegation of the failure to materially comply with any provision of this Agreement, the Parties may pursue any remedy available to them under this Agreement or otherwise without pursuing the dispute resolution process set forth herein.

The phrase "failure to materially comply with any provision of this Agreement" shall be defined to mean any deficiency of either Party's performance which, either as a standalone event, or as an aggregation of multiple events over time that constitutes a substantial and continuing violation of the warranties of this Agreement including those required by the RFP and those contained in Contractor's Offering; or threatens the public safety of those citizens and entities served by _____. _____ has retained and relies on the performance of Contractor in performing its obligations hereunder specifically because Contractor has declared its expertise and held itself out as having expertise and experience as claimed in its proposal and which is expected within its field.

Subcontractors

It is understood and agreed that all Subcontractors must be approved by the State. Throughout the Contract term, the Contractor must furnish a written copy of all subcontracts, including

subsequent amendments thereto, to the State and certify the completeness thereof of all executed subcontracts or third-party agreements, which support the Contractor's ability to furnish the products and services for this project. In the context of this section, the phrases "certify the completeness thereof" and "certify the terms of third party agreements" shall mean that the Contractor has fully disclosed all terms and conditions of the aforesaid subcontracts and/or third party agreements and will affirmatively disclose to the State any amendments thereto which occur subsequent to the certification. The State's failure to receive or request such agreements shall not constitute a waiver of these rights.

Additionally, to the extent that the Contractor identifies as a proposed subcontractor in its' proposal or under this PSCTS Contract an entity which has independently executed a contract with the State of New York for similar services or products as those to be provided through Contractor under this PSCTS Contract,, and such subcontractor's direct State contract imposes obligations, terms or conditions on the subcontractor which are more beneficial to the State than those set forth in the Contract resulting from this procurement as to such subcontractor's responsibilities under the PSCTS, the State reserves the right to:

- a. require the Contractor to incorporate into the PSCTS Contract such more beneficial terms and conditions, and
- b. require the Contractor to deliver to the State subcontractor's written agreement to incorporate and honor such additional or beneficial terms to its obligations to the State under the PSCTS Contract, and
- c. withhold the approval of subcontractor pending receipt by the State of written agreements complying with a and b, above.

In the alternative, the State reserves the right to delete any portion of work to be performed by such subcontractor from the scope of the PSCTS and to acquire such services under the independent State contract where the State determines it would be more advantageous to acquire such products or services directly.

The rights and remedies provided in this Agreement shall not be exclusive and are in addition to any other rights and remedies provided by law.

State's Right to Assign Contract

The State may at its sole option assign this Agreement to any other agency of the State of New York.

Entire Agreement and Survival

This Agreement constitutes the entire Agreement between the Parties hereto and no statement, promise, condition, understanding, inducement or representation, oral or written, expressed or implied, which is not contained or referenced herein shall be binding or valid. The terms, provisions, representations and warranties contained in this Agreement shall survive performance hereunder. This Agreement shall not be changed, modified or altered in any manner, other than as provided in this Agreement, except by a written instrument executed by the Parties and approved by the Department of Law General and Office of the State Comptroller.

IN WITNESS WHEREOF, the Parties therefore hereby execute their mutual Agreement to the terms of this Agreement, bearing New York State Comptroller's Contract Number _____. This Agreement constitutes a binding Agreement between the Parties as of the day and year indicated below that the approval of the Comptroller of the State of New York or staff of the Office of the State Comptroller (OSC) designated for such purpose was received. The Parties further agree that, where Contractor is asked to execute any original copies of this signature page along with a complete original copy of this Agreement, that the approved signature page will be affixed by DCJS upon its receipt of final approval of the Comptroller of the State of New York or staff of the Office of the State Comptroller (OSC) designated for such purpose, to additional copies of this Agreement which conform exactly to the complete original copy as submitted by Contractor and executed simultaneously therewith.

Contractor

Date: _____

By:

[title]

Date: _____

STATE AGENCY NAME

By:

[title]

STATE OF _____ }
 _____ } SS
 COUNTY OF _____ }

Notary Public

Approved:

This Page Intentionally Blank

Attachment 21

State Consultant Services Contractors Annual Employment Report Addendum

Intentionally Blank

ADDENDUM ACKNOWLEDGING FORM B

Pursuant to State Finance Law §163(4)(g), Vendor agrees to annually submit Form B, State Consultant Services Contractor's Annual Employment Report to DCJS, the NYS Office of the Comptroller and NYS Department of Civil Service. A copy of Form B and instructions are attached.

The State Consultant Services Contractor's Annual Employment Report (Form B) must be submitted each year the contract is in effect and will capture actual employment data for the most recently concluded fiscal year April 1, 20__ to March 31, 20__. The first report is due May 15, 20__ and thereafter May 15th of each year.

The Vendor agrees to simultaneously report such information to the NYS Division of Criminal Justice Services, the NYS Office of the State Comptroller and the NYS Department of Civil Service as designated below:

NYS Division of Criminal Justice Services Attn: Office of Financial Services Alfred E. Smith Office Building, 10 th Floor 80 South Swan Street Albany, NY 12210-8001	Office of the State Comptroller Bureau of Contracts 110 State Street, 11 th Floor Albany, NY 12236 Attn: Consultant Reporting By fax: (518) 474-8030 or (518) 473-8808	NYS Department of Civil Service Attn: Consultant Reporting Empire State Plaza Swan Street Bldg. 1 Albany, NY 12210

 Authorized Signature

 Date

 Name (Please print)

 Title (Please print)
ACKNOWLEDGEMENT CLAUSE

State of New York)

) ss.:

County of Albany)

On this ____ day of _____, 20__, before me personally came _____, to me known, who being duly sworn, deposes and says that (s)he is the _____ of the _____, the entity which executed the instrument; that (s)he was authorized by and did execute the same at the direction of said entity and that (s)he signed his/her name thereto.

 Notary Public

FORM B	OSC Use Only: Reporting Code: _____ Category Code: _____
State Consultant Services Prime Contractor's Annual Employment Report Report Period: April 1, to March 31,	

Contracting State Agency Name: <u>Division of Criminal Justice Svcs</u> Agency Code: <u>01490</u>			
Contract Number: _____			
Contract Term: <u> / / </u> to <u> / / </u>			
Contractor Name: _____			
Contractor Address: _____			
Description of Services Being Provided: _____			
Scope of Contract (Choose one that best fits): Analysis ☐ Evaluation ☐ Research ☐ Training ☐ Data Processing ☐ Computer Programming ☐ Other IT consulting ☐ Engineering ☐ Architect Services ☐ Surveying ☐ Environmental Services ☐ Health Services ☐ Mental Health Services ☐ Accounting ☐ Auditing ☐ Paralegal ☐ Legal ☐ Other Consulting ☐			
Employment Category	Number of Employees	Number of Hours Worked	Amount Payable Under the Contract
Total this page			
Grand Total			

Name of person who prepared this report: _____	
Preparer's Signature: _____	
Title: _____	Phone #: _____
Date Prepared: <u> / / </u>	

Use additional pages if necessary)

Page of

This Page Intentionally Blank

Attachment 22

FBI CJIS Security Addendum

Intentionally Blank

APPENDIX H SECURITY ADDENDUM

The following pages contain the legal authority, purpose, and genesis of the Criminal Justice Information Services Security Addendum (H2-H4); the Security Addendum itself (H5-H6); and the Security Addendum Certification page (H7).

**FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM**

**Legal Authority for and Purpose and Genesis of the
Security Addendum**

Traditionally, law enforcement and other criminal justice agencies have been responsible for the confidentiality of their information. Accordingly, until mid-1999, the Code of Federal Regulations Title 28, Part 20, subpart C, and the National Crime Information Center (NCIC) policy paper approved December 6, 1982, required that the management and exchange of criminal justice information be performed by a criminal justice agency or, in certain circumstances, by a noncriminal justice agency under the management control of a criminal justice agency.

In light of the increasing desire of governmental agencies to contract with private entities to perform administration of criminal justice functions, the FBI sought and obtained approval from the United States Department of Justice (DOJ) to permit such privatization of traditional law enforcement functions under certain controlled circumstances. In the Federal Register of May 10, 1999, the FBI published a Notice of Proposed Rulemaking, announcing as follows:

1. Access to CHRI [Criminal History Record Information] and Related Information, Subject to Appropriate Controls, by a Private Contractor Pursuant to a Specific Agreement with an Authorized Governmental Agency To Perform an Administration of Criminal Justice Function (Privatization). Section 534 of title 28 of the United States Code authorizes the Attorney General to exchange identification, criminal identification, crime, and other records for the official use of authorized officials of the federal government, the states, cities, and penal and other institutions. This statute also provides, however, that such exchanges are subject to cancellation if dissemination is made outside the receiving departments or related agencies. Agencies authorized access to CHRI traditionally have been hesitant to disclose that information, even in furtherance of authorized criminal justice functions, to anyone other than actual agency employees lest such disclosure be viewed as unauthorized. In recent years, however, governmental agencies seeking greater efficiency and economy have become increasingly interested in obtaining support services for the administration of criminal justice from the private sector. With the concurrence of the FBI's Criminal Justice Information Services (CJIS) Advisory Policy Board, the DOJ has concluded that disclosures to private persons and entities providing support services for criminal justice agencies may, when subject to appropriate controls, properly be viewed as permissible disclosures for purposes of compliance with 28 U.S.C. 534.

We are therefore proposing to revise 28 CFR 20.33(a)(7) to provide express authority for such arrangements. The proposed authority is similar to the authority that already exists in 28 CFR 20.21(b)(3) for state and local CHRI systems. Provision of CHRI under this authority would only be permitted pursuant to a specific agreement with an authorized governmental

agency for the purpose of providing services for the administration of criminal justice. The agreement would be required to incorporate a security addendum approved by the Director of the FBI (acting for the Attorney General). The security addendum would specifically authorize access to CHRI, limit the use of the information to the specific purposes for which it is being provided, ensure the security and confidentiality of the information consistent with applicable laws and regulations, provide for sanctions, and contain such other provisions as the Director of the FBI (acting for the Attorney General) may require. The security addendum, buttressed by ongoing audit programs of both the FBI and the sponsoring governmental agency, will provide an appropriate balance between the benefits of privatization, protection of individual privacy interests, and preservation of the security of the FBI's CHRI systems.

The FBI will develop a security addendum to be made available to interested governmental agencies. We anticipate that the security addendum will include physical and personnel security constraints historically required by NCIC security practices and other programmatic requirements, together with personal integrity and electronic security provisions comparable to those in NCIC User Agreements between the FBI and criminal justice agencies, and in existing Management Control Agreements between criminal justice agencies and noncriminal justice governmental entities. The security addendum will make clear that access to CHRI will be limited to those officers and employees of the private contractor or its subcontractor who require the information to properly perform services for the sponsoring governmental agency, and that the service provider may not access, modify, use, or disseminate such information for inconsistent or unauthorized purposes.

Consistent with such intent, Title 28 of the Code of Federal Regulations (C.F.R.) was amended to read:

§ 20.33 Dissemination of criminal history record information.

- a) Criminal history record information contained in the Interstate Identification Index (III) System and the Fingerprint Identification Records System (FIRS) may be made available:
 - 1) To criminal justice agencies for criminal justice purposes, which purposes include the screening of employees or applicants for employment hired by criminal justice agencies.
 - 2) To noncriminal justice governmental agencies performing criminal justice dispatching functions or data processing/information services for criminal justice agencies; and
 - 3) To private contractors pursuant to a specific agreement with an agency identified in paragraphs (a)(1) or (a)(6) of this section and for the purpose of providing services for the administration of criminal justice pursuant to that agreement. The agreement must incorporate a security addendum approved by the Attorney General of the United

States, which shall specifically authorize access to criminal history record information, limit the use of the information to the purposes for which it is provided, ensure the security and confidentiality of the information consistent with these regulations, provide for sanctions, and contain such other provisions as the Attorney General may require. The power and authority of the Attorney General hereunder shall be exercised by the FBI Director (or the Director's designee).

This Security Addendum, appended to and incorporated by reference in a government-private sector contract entered into for such purpose, is intended to insure that the benefits of privatization are not attained with any accompanying degradation in the security of the national system of criminal records accessed by the contracting private party. This Security Addendum addresses both concerns for personal integrity and electronic security which have been addressed in previously executed user agreements and management control agreements.

A government agency may privatize functions traditionally performed by criminal justice agencies (or noncriminal justice agencies acting under a management control agreement), subject to the terms of this Security Addendum. If privatized, access by a private contractor's personnel to NCIC data and other CJIS information is restricted to only that necessary to perform the privatized tasks consistent with the government agency's function and the focus of the contract. If privatized the contractor may not access, modify, use or disseminate such data in any manner not expressly authorized by the government agency in consultation with the FBI.

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A-130 as “security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.”

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.

1.00 Definitions

1.01 Contracting Government Agency (CGA) - the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.

1.02 Contractor - a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

2.00 Responsibilities of the Contracting Government Agency.

2.01 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. The acknowledgement may be signed by hand or via digital signature (see glossary for definition of digital signature).

3.00 Responsibilities of the Contractor.

3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed and all subsequent versions), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

4.00 Security Violations.

4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

4.02 Security violations can justify termination of the appended agreement.

4.03 Upon notification, the FBI reserves the right to:

- a. Investigate or decline to investigate any report of unauthorized use;
- b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CJA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

5.00 Audit

5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

6.00 Scope and Authority

6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.

6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

6.04 This Security Addendum may only be modified by the FBI, and may not be modified by the parties to the appended Agreement without the consent of the FBI.

6.05 All notices and correspondence shall be forwarded by First Class mail to:

Assistant Director

Criminal Justice Information Services Division, FBI

1000 Custer Hollow Road

Clarksburg, West Virginia 26306

**FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM**

CERTIFICATION

I hereby certify that I am familiar with the contents of (1) the Security Addendum, including its legal authority and purpose; (2) the NCIC Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20, and agree to be bound by their provisions.

I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which a government agency has entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

Printed Name/Signature of Contractor Employee

Date

Printed Name/Signature of Contractor Representative

Date

Organization and Title of Contractor Representative

This Page Intentionally Blank

Attachment 23

Proposed Fixed Purchase Price - Mandatory Base System

Intentionally Blank

Attachment 23
Proposed Fixed Purchase Price - Mandatory Base System

	Fixed Purchase Price
Cost Breakdown:	
a. Software License Fee	
b. Development and Implementation Services	
c. Other	
d. Proposed Fixed Purchase Price (sum of above costs)	<u><u>0</u></u>

This Page Intentionally Blank

Attachment 24

Maintenance and Support Price - Mandatory Base System

Intentionally Blank

This Page Intentionally Blank

Attachment 25

Optional Licensing and Professional Services Price List

Intentionally Blank

Attachment 25

Optional Licenses and Professional Services Price List

Provide pricing for optional licenses that would be available to NYS at its discretion. Include all licensing models, including per user and enterprise licensing if available.

1. Optional Licenses	Price Basis	License Cost	Support and Maintenance Cost	Total
a.	Per User			
b.	Enterprise			
c.	Other			
d. least expensive cost for license and support/maintenance for an additional 1,000 users				0

Provide pricing for professional services that would be available to DCJS at its discretion. Include all possible titles of staff (e.g., developers and engineers) in the list. Compute the Average Hourly Fee by dividing the sum of all Hourly Fees by the number of titles in the Offerers' list.

2. Professional Services	Price Basis	Fee (\$ U.S.)
a.	Hourly Fee	
b.	Hourly Fee	
c.	Hourly Fee	
d.	Hourly Fee	
e.	Hourly Fee	
f.	Hourly Fee	
g.	Hourly Fee	
h. Average Hourly Fee		

This Page Intentionally Blank

Attachment 26

**Total Proposed Cost for Offerer's Mandatory
Base System for Initial 10 Year Contract
Period**

Intentionally Blank

Attachment 26

Total Proposed Cost for Offerer's Mandatory Base System for Initial 10 Year Contract Period

and, for evaluation scoring purposes only, assumed optional licenses and professional services

1. Price Component	2. Proposed Price (\$US)	3. Estimated Hours	4. Extended Price
a. Fixed Purchase Price - Mandatory Base System (source: Attachment 23, line d.)			\$ -
b. Maintenance and Support Cost - Mandatory Base System (source: Attachment 24, Total)			\$ -
c. Least expensive cost model for Optional Licenses and Support/Maintenance for 1,000 additional users (source: Attachment 25, line 1.d, Total Column)			\$ -
d. Estimated Cost for Optional Professional Services (source: Attachment 25, line 2.h.		1,000	\$ -
e. Total Cost (sum of a, b, c and d above)			\$ -

This Page Intentionally Blank

Attachment 27

Proposed Fixed-Price Milestone Deliverable Payment Schedule

Intentionally Blank

Attachment 27

Proposed Fixed-Price Milestone Deliverable Payment Schedule

Provide the Offerer's fixed price for all deliverables defined within the Project Plan including, but not limited to, software and services. The deliverables and associated payment schedule submitted by each Offerer must match its submitted Project Plan. Each deliverable must have a delivery date and payment amount associated with it and the total payment amount of the schedule must be summed and may not exceed twenty five (25) percent of the Offerer's proposed fixed-price purchase price. (Attachment 23, line d.). Additionally, Offerer must propose acceptance criteria associated with each proposed milestone deliverable payment. DCJS reserves the right to negotiate the Offerer requested payment schedule and acceptance criteria, should DCJS find unacceptable the schedule as proposed.

Milestone Deliverable - Offerer to propose	Delivery Date	Payment Amount (\$US)
Deliverable 1		
Deliverable 2		
Deliverable 3		
Deliverable 4		
Deliverable 5		
Proposed Total Deliverable Payment Schedule (sum of above costs)		\$ -

Proposed Acceptance Criteria:

- Deliverable 1
- Deliverable 2
- Deliverable 3
- Deliverable 4
- Deliverable 5

This Page Intentionally Blank

Attachment 28

Detailed Optional Features Price List

This Page Intentionally Blank

Attachment 28
Detailed Optional Features Price List

The pricing of optional features and services, as detailed in RFP 3.1.D, shall be proposed by the Offerer so that pricing is known in advance in the event that DCJS chooses to acquire additional capabilities throughout the term of the contract. Provide an entry in this table providing any incremental costs associated with each optional feature. If the offerer intends to propose any maintenance costs with an optional feature, include that cost in the appropriate column.

Customization Costs (\$US)				
Number	Description	COTS	No Proposal	Incremental Software License Fee Cost
1				Incremental Services Cost
2				Total Optional Feature Cost
3				Monthly Maintenance Cost *
TOTALS				

* After warranty period ends which will be twelve (12) months after the feature is migrated to production.

This Page Intentionally Blank

Attachment 29

Optional Services Price List

Intentionally Blank

Attachment 29

Optional Services Price List

Provide pricing for optional services that would be available to NYS at its discretion. Include services such as conversion and training (hourly or perhaps other scenarios such as per class).

	Price Basis	Price

1. Conversion Service		

2. Training		

3. Other		