U. S. Department of Justice
Federal Bureau of Investigation
Criminal Justice Information Services Division

Criminal Justice Information Services (CJIS) Law Enforcement National Data Exchange (N-DEx)

Policy and Operating Manual

Version: 2.1
Document Date: August 9, 2012
N-DEx-DOC-09172-2.1

The N-DEx Policy and Operating Manual supersedes all pre-existing policy documentation and is the sole source for policy matters for the N-DEx system.

Change Description Form

Version / Revision	Change Description	Changed By	Date	Approved By
Initial Draft	N-DEx Policy and Operating Manual	Patrick Ringer	4/5/2011	ISNOTF
ISNOTF Approved Draft	Update to N-DEx Policy and Operating Manual	Darrin Paul	4/13/2011	INSH
INSH Approved Draft	Adoption of N-DEx Policy and Operating Manual	Darrin Paul	5/11/2011	APB Executive Committee
Version 2.0	Policy Up-date	B.T. Stout	5/30/2012	INSH Chairman
Version 2.1	Policy Up-date	Amber Fazzini	8/9/2012	INSH Chairman

LAW ENFORCEMENT NATIONAL DATA EXCHANGE (N-DEx)

POLICY AND OPERATING MANUAL

Table of Contents

1.0 INTRODUCTION

1.1 Purpose

1.1.1 Law Enforcement National Data Exchange (N-DEx) Mission: To provide law enforcement with a powerful new investigative tool to search, link, analyze and share law enforcement/criminal justice information such as, incident/case reports, booking and incarceration data, and parole and/or probation data on a national basis to a degree never before possible.

1.1.2 N-DEx Vision: To share complete, accurate, timely, and useful law enforcement/criminal justice information across jurisdictional boundaries and to provide new investigative tools that enhance the nation's ability to fight crime and terrorism.

1.1.3 Scope of N-DEx policy: The N-DEx Policy and Operating Manual applies to all entities accessing N-DEx. N-DEx information shall be used only for the purpose indicated by the Use Code and used consistently with the coordination required by the Advanced Permission Requirement (confirming the terms of N-DEx information use). Any subsequent use of N-DEx information inconsistent with the original Use Code or the previously conducted Advanced Permission Requirement requires re-satisfaction of the Advanced Permission Requirement.

1.1.4 The N-DEx Policy and Operating Manual integrates presidential directives, federal laws, Federal Bureau of Investigation (FBI) directives, and the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB) decisions to provide criminal justice agencies with a minimum set of policy and procedural requirements for participating in N-DEx and to protect and safeguard criminal justice information. This minimum set of requirements ensures continuity of N-DEx operation and information security.

1.1.5 The N-DEx Policy and Operating Manual may be used as the sole policy and operating manual for N-DEx participating agencies. A participating agency may complement the N-DEx Policy and Operating Manual with agency specific policy and operating procedures, or the participating agency may develop their own stand-alone policy and operating manual; however, the N-DEx Policy and Operating Manual shall always be the minimum standard and participating agencies may augment, or increase the standards, but shall not detract from the N-DEx Policy and Operating Standards.

1.1.6 The N-DEx Policy and Operating Manual applies to all entities with access to, or who operate in support of, N-DEx services and information. This policy manual is subject to change as a result of presidential directives, federal laws, FBI directives, and CJIS APB decisions. The terms of any policy and procedural change preempt any existing inconsistency contained herein.

1.1.7 The N-DEx Policy and Operating Manual is an unrestricted document and can be shared without limitation.

1.2 Operational Framework

1.2.1 The N-DEx system is a system managed within the framework of the CJIS System of Services and identified within the CJIS systems User Agreement.

1.2.2 Participating agencies and users must adhere to the *CJIS Security Policy*.

1.2.3 The N-DEx system stores vast amounts of criminal justice information which may be instantly retrieved by and/or furnished to any authorized agency.

1.2.4 N-DEx is restricted to documented criminal justice information obtained by criminal justice agencies in connection with their official duties administering criminal justice.

1.2.5 Within the context of N-DEx, leveraging refers to the capability to access National Crime Information Center (NCIC) and Interstate Identification Index (III) via a N-DEx search. Leveraging is only available if both the CJIS Systems Agency (CSA) and User Administrator (UA) authorize and enable this capability.

1.2.6 N-DEx will not contain criminal intelligence data as defined by Title 28, Code of Federal Regulations (C.F.R.), Part 23.

1.2.7 In accordance with the *CJIS Security Policy* and consistent with Title 28, C.F.R., Part 20, Subpart A, N-DEx system access is restricted to "criminal justice agencies" and agencies performing the "administration of criminal justice."

1.2.8 N-DEx is an on-line real-time program and records are constantly being updated; therefore, record information can change at any time.

1.2.9 N-DEx is the national enhanced pointer and data discovery system for SBU, law enforcement sensitive, and Controlled Unclassified Information (CUI) class criminal justice data.

1.2.10 N-DEx is a fee free, secure, nationwide, computerized information sharing system established to fill an identified gap in the CJIS System of Services.

1.2.11 The N-DEx Program is a cooperative endeavor of local, state, tribal, and federal law enforcement/criminal justice entities, in which each entity is participating under its own legal status, jurisdiction and authorities. All N-DEx operations will be based upon the legal status, jurisdiction and authorities of individual participants. N-DEx is not intended, and shall not be deemed, to have any independent legal status.

1.2.12 Agencies shall participate in N-DEx in accordance with their own individual legal status, jurisdiction, restrictions, and authorities.

1.2.13 Participating agencies contribute information to N-DEx with an express promise of confidentiality.

1.2.14 N-DEx participants shall contribute or allow access to information via N-DEx, and agrees to permit the access, dissemination, and/or use of such information by other parties pursuant to the provisions of this policy. The record owning agency has the sole responsibility and accountability for ensuring that it is not constrained from permitting this access by any laws, regulations, policies, or procedures.

1.2.15 N-DEx is not created pursuant to a single federal statute; rather, N-DEx is the FBI's response to the criminal justice community's request to answer the challenge of information sharing.

1.2.16 All inquiries regarding the N-DEx system should be addressed to the FBI, CJIS Division, via e-mail: ndex@leo.gov; via telephone (304) 625-HELP [4357]: or via mail; Attention: N-DEx Program Office, Module B-3, 1000 Custer Hollow Road, Clarksburg, WV 26306-0153.

1.3 Data Use

1.3.1 The N-DEx system shall be used in accordance with the policies in this document and those of the leveraged CJIS System of Services operating procedures or policies. The CSA shall ensure N-DEx participating agencies have procedures to comply with the policies in this document and those of the leveraged CJIS system as a part of enabling user agency access of leveraged services, e.g., procedures to engage hit confirmation and the placing of a "locate" in accordance with NCIC policy.

1.3.2 An N-DEx result indicates that criminal justice information may exist.

1.3.3 System Access: N-DEx contains criminal justice information obtained by criminal justice agencies in connection with their official duties administering criminal justice, and N-DEx system access is restricted to criminal justice agencies and agencies performing the administration of criminal justice. Only the following agencies are authorized to access N-DEx based on the agency type Originating Agency Identifier (ORI) value as indicated by the 9th character:

1.3.3.1 Law Enforcement Agencies

- Law enforcement agencies possessing 9th character ORIs of 0 - 9 (numeric values) e.g., police, sheriff, etc.

1.3.3.2 Criminal Justice Agencies

- Prosecuting Attorney's Offices –ORIs end in an "A." This includes District Attorney's Offices, Attorney General's Offices, etc.

- Pretrial service agencies and pretrial release agencies – ORIs end in a "B."

- Correctional Institutions ORIs end in a "C." This includes jails, prisons, detention centers, etc.

- Nongovernmental railroad or campus police departments qualifying for access to III – ORIs end in an "E."

- Probation and Parole Offices – ORIs end in a "G."

- INTERPOL – ORIs end in an "I." As a foreign criminal justice agency, INTERPOL shall be a Limited System Participant. Local, state, and tribal criminal justice agency data shall not be shareable with limited system participants.

- Courts and Magistrates Offices – ORIs end in a "J."

- Custodial facilities in medical or psychiatric institutions and some medical examiners' offices which are criminal justice in function – ORIs end in an "M."

- Regional dispatch centers that are criminal justice agencies or noncriminal justice governmental agencies performing criminal justice dispatching functions for criminal justice agencies – ORIs end in an "N."

- Local, county, state, or federal agencies that are classified as criminal justice agencies by statute but do not fall into one of the aforementioned categories – ORIs end in a "Y."

1.3.4 Acceptable System Use: Personnel engaged in the following activities may be granted access by the CSA consistent with state laws:

1.3.4.1 Law enforcement investigations, i.e., to further investigations of criminal behavior based on prior identification of specific criminal activity by an agency with a statutory ability to perform arrest functions.

1.3.4.2 Pretrial release investigation, i.e., to obtain information about recently arrested defendants for use in deciding whether conditions are to be set for defendants' release prior to trial, monitor a defendant's compliance with his/her conditions of release during pretrial period, and identify offenses pending adjudication.

1.3.4.3 Intake investigation, i.e., to conduct prisoner classification and offender risk assessments to safely manage the correction population.

1.3.4.4 Correctional institution investigation, i.e., to identify and suppress criminal suspects and criminal enterprise organizations operating within correctional systems, prepare for the prosecution of crimes committed within a correctional institution, conduct criminal apprehension efforts of prison escapees, ensure inmates cannot continue their criminal activities through misuse of visitation or communication privileges, monitor out source supervision and treatment progress, conduct offender travel permit investigations, prepare for prisoner transfer, and conduct pre-release investigation to determine reentry requirements and facilitate release notification.

1.3.4.5 Pre-sentence investigation, i.e., to identify the risk of reoffense, flight, community, officer and victim safety, identify law enforcement contact not resulting in arrest, identify offenses pending adjudication, and ensure illicit income is not used for bail, bond, or criminal defense.

1.3.4.6 Supervision investigation, i.e., to identify incident information (i.e. personal conduct, contact with LEAs, offenses, gang affiliations, known associates, employment, etc.) constituting a violation of release or supervision conditions, prepare and investigate interstate transfer of adult offenders, facilitate concurrent supervision, conduct risk and needs assessments, facilitate apprehension of absconders, and identify offenses pending adjudication.

1.3.4.7 Data administration/management, i.e., to perform administrative role responsibilities and conduct searches of record owner contributed data as a part of internal review by a record owner. Responses for this purpose may not be disseminated for any other reason and are limited to that agency's portion of N-DEx contributed records.

1.3.4.8 Training, i.e., to educate users on the policies, services and capabilities of the N-DEx system utilizing authentic criminal justice information submitted to N-DEx by criminal justice agencies.

Training is considered to be an acceptable use of N-DEx, so long as it does not include curiosity searches, browsing, or self-queries.

1.3.5 "On behalf of" Log Retention: Each N-DEx search shall clearly identify the N-DEx user, requesting agency, and any individual the search was made "on behalf of" if known at the time the search was conducted. Identification shall take the form of a unique identifier, which shall be captured and maintained in a transaction log, with the identifier remaining unique, for a minimum of one year. While N-DEx supports this logging requirement through the N-DEx Portal, entities accessing N-DEx data through a trusted connection must independently maintain these logs and are

encouraged to automate the logging requirement. Using the search reason field to capture "on behalf of" meets the requirement of a log."

1.3.6 All users are required to provide a search reason. While the Use Code provides some lead information, it only provides a minimal audit trail. Requiring the reason for all searches will ensure N-DEx searches are conducted for authorized uses and use codes are correctly applied. It is recommended unique information, e.g., incident number, arrest transaction number, booking number, project name, description, etc., be entered to assist the user in accounting for appropriate system use for each transaction. This information shall be captured and maintained in a transaction log for a minimum of one year.

1.3.7 Authorized Pre-Permission Use: N-DEx information may be viewed, output, or discussed without advance authorization of the record owning agency, within the record-requesting agency or another agency, if the other agency is an authorized recipient of such information by virtue of meeting the requirements for N-DEx access and is being serviced by the record-requesting agency. However, any recipient of N-DEx data must obtain advanced permission from the record-owning agency prior to acting upon any data obtained through N-DEx.

1.3.8 Advanced Permission Requirement: Terms of N-DEx information use must be obtained from the record-owning agency prior to reliance or action upon, or secondary dissemination. N-DEx information may only be relied or acted upon, or secondarily disseminated within the limitations specified by the record-owning agency. Reliance or action upon, or secondary dissemination of N-DEx information beyond the original terms requires further permission from the record owning agency. The use or inclusion of N-DEx information in the publication or preparation of charts, presentations, official files, analytical products or other documentation, to include, use in the judicial, legal, administrative, or other criminal justice process, etc., specifically requires advanced permission.

1.3.9 Verification Requirement: N-DEx information must be verified with the record-owning agency for completeness, timeliness, accuracy, and relevancy prior to reliance upon, action, or secondary dissemination.

1.3.10 Information returned specifically from an N-DEx leveraged CJIS System of Services system may only be used in accordance with the policies governing those specific systems.

1.3.11 Immediate use of N-DEx information can be made without the advanced permission of the record owning agency if there is an exigent circumstance - an emergency situation requiring swift action to prevent imminent danger to life or serious damage to property, or to forestall the imminent escape of a suspect, or destruction of evidence. The record-owning agency shall be immediately notified of any use made as a result of exigent circumstances.

1.3.12 Participating agencies are encouraged to consider how they may wish to account for use authorization requests and concurrences. While N-DEx does not systematically support nor require a log to be maintained, agencies are encouraged to consider how the advanced permission, verification, and data provision may be documented within their own organization.

1.4 Responsibility for Records

1.4.1 Record-owning agencies that make available records in the N-DEx system are responsible for their timeliness, accuracy, and completeness. For further explanation of timeliness, accuracy, and completeness, see section 2.5 Maintaining The Integrity of N-DEx Records.

1.4.2 Each record-owning agency controls how and with whom their data is shared, thus retaining responsibility, control, and ownership.

1.4.3 Agency-Configurable Data Sharing Controls: N-DEx is designed to allow record-owning agencies to protect their data in accordance with the laws and policies that govern dissemination and privacy for their jurisdictions. All data is presumed sharable unless the record-owning agency restricts data access, in accordance with their sharing policy. N-DEx enables data sharing at the following data item (i.e. reports) dissemination criteria values:

1.4.3.1 Green: Data is viewable.

1.4.3.2 Yellow: Data consists of record ID and record-owning agency Point of Contact (POC) information. To obtain access, contact the record-owning agency.

1.4.3.3 Red: Data is not viewable.

1.4.3.4 Record-owning agencies shall have the ability to configure sharing policy based on agency, agency type, individual users, or data characteristics to create exception groups for their data. Thus, an N-DEx record may be red to one user, yellow to a second, and green to a third. Record-owning agencies are encouraged to submit records using the green value; however if an agency must submit records using the red or yellow values, they are encouraged to make their records green for their agency to realize the full benefit of automatic entity integration, data correlation, and other tools within N-DEx, including the creation of subscriptions.

1.4.4 Pursuant to Executive Order 12958 as amended, *Classified National Security Information*, N-DEx is designated as an unclassified system. Record-owning agencies shall ensure that data contributed to and/or exchanged by N-DEx is unclassified and free of classified national security information. Information contributed to N-DEx resides on a server(s) located in FBI controlled space,

containing SBU and CUI from contributing agencies with established formal agreements.

1.4.5 All participating agencies whether contributing information to N-DEx or leveraging N-DEx shall access the N-DEx server(s) and functionality via secure internet connections (as defined by the *CJIS Security Policy*) or via the FBI's CJIS Wide Area Network.

1.4.6 The FBI CJIS Division, as manager of N-DEx, helps maintain the integrity of the system through:

1.4.6.1 Automatic computer checks which reject records with common types of errors in data.

1.4.6.2 Pre-data ingestion analysis and data inspection.

1.4.6.3 On-going manual quality control checks by FBI personnel.

1.4.6.4 Automated tool support, e.g., conformance testing assistant, for construction of data submissions.

1.4.6.5 System generated error reports for viewing by the record-owning Source Data Administrator (SDA) and CSA.

1.4.6.6 Monitoring and automated logging of all successful and unsuccessful logon attempts where CJIS is the identity provider, file access, correlations, and transaction types, regardless of access means.

1.4.7 The CSA shall ensure criminal justice agencies that have users connecting to N-DEx through methods that do not permit the capture of N-DEx user information have the ability to generate reports upon request of the CSA and/or N-DEx PO. These reports may be used to audit system access and use.

1.5 System Description

1.5.1 Full system participants are local, state, tribal, and federal criminal justice agencies throughout the United States, District Of Columbia, United States territories.

1.5.2 Limited system participants are foreign criminal justice agencies. Local, state, and tribal criminal justice agency data shall not be shareable with limited system participants, i.e. foreign criminal justice agencies.

1.5.2.1 N-DEx is the technical mechanism to bi-directionally share federal government unclassified criminal justice information with foreign partners, e.g., Australian Federal Police, New Zealand Police, and United Kingdom Serious Organized Crime Agency.

1.5.3 Data contributed to the N-DEx system must meet the criteria established for the particular type of record involved as identified in the N-DEx Information Exchange Package Documentation (IEPD).

1.5.4 N-DEx has the ability to leverage other CJIS System of Services. The capability to leverage additional CJIS System of Services using N-DEx is discretionary with each CSA.

1.5.5 In accordance with the *CJIS Security Policy*, Criminal Justice Information (CJI) shall refer to all FBI CJIS provided data necessary for criminal justice agencies to perform their missions. Such information shall consist of, but not be limited to biometric, identity history, biographic, property, and case/incident history data.

1.5.6 Data contributed and/or exchanged via N-DEx is CJI, which contains Personally Identifiable Information, e.g., names, social security numbers, etc., as well as, non-identifying descriptive information e.g., offense location, weapon involved, etc., and may contain criminal history record information as defined in Title 28, C.F.R., Part 20. The collection, storage, and dissemination of information shall comply with all applicable laws and regulations.

1.5.7 In accordance with the *CJIS Security Policy*, an information exchange agreement, i.e., a formal agreement specifying security controls must be signed before exchanging criminal justice information. Formal agreements may take the form of user agreements, management control agreements, CJIS security addendum, or any other document that meets the requirements articulated in the *CJIS Security Policy*.

1.6 Policy Management

1.6.1 The CJIS APB, established by Title 28, C.F.R., Part 20.35, recommends general policy to the FBI Director with respect to the philosophy, concept, and operational principles of the N-DEx system. In its deliberations, the APB places particular emphasis on system security; and rules, regulations, and procedures to maintain the integrity of CJIS System of Services and criminal justice information.

1.6.2 Detailed information on the operation of the APB process can be found within the *Bylaws for the Criminal Justice Information Services Advisory Policy Board and Working Groups*.

1.6.3 In accordance with the *CJIS Security Policy*, the CJIS Systems Officer (CSO) or designee shall ensure a Terminal Agency Coordinator (TAC) is designated within each agency that has devices accessing CJIS systems. The TAC serves as the POC for the CSO at the local agency for matters relating to CJIS information access. The TAC administers CJIS systems programs with the local agency and oversees the agency's compliance with CJIS systems policies.

1.6.4 The CSO or designee shall ensure an N-DEx Agency Coordinator (NAC) is designated within each agency which accesses N-DEx. The NAC serves as the POC for the CSO at the local agency for matters relating to N-DEx. The NAC administers N-DEx within the local agency and oversees the agency's compliance with N-DEx system policies. The NAC may also be the agency's TAC. An agency may change its NAC at any time, but must notify the CSA in writing of the change. The following N-DEx roles may be performed by the CSO, or delegated to the NAC or other appropriate personnel within the CSA or N-DEx agency. It is recommended an alternate be assigned as a back-up to assist with performing the administrative duties in case of emergency or personnel changes. One individual may perform all administrative roles, or the roles may be assigned to several individuals.

1.6.4.1 User Administrator (UA) – Responsible for administering user permissions within assigned agencies. These duties may include establishing, managing, or removing user access and roles, as well as verifying and establishing access to leveraged CJIS System of Services. The N-DEx PO enables the UA capability.

1.6.4.2 Audit/Security Administrator (SA) – Responsible for either managing the Data and User Auditor and/or performing these roles. The Data and User auditors can be the same individual and shall be members of the contributing or record-owning agency. The respective CSA shall have the capability to utilize the audit functionality for all agencies under its authority.

- Data Auditor - authorized to manage audit reports regarding which agencies have accessed the record owner's data.
- User Auditor - authorized to manage audit reports regarding searches performed, collaboration postings/retrievals completed, etc., of all users within the assigned agency.

1.6.4.3 Source Data Administrator (SDA) – Responsible for establishing and managing the agency's configurable data sharing controls and submitting data to N-DEx for assigned record-owning agency(ies). If the record-owning agency chooses to submit Uniform Crime Reporting / National Incident Based Reporting System (NIBRS) data via N-DEx, the SDA's role is expanded to include responsibilities for managing the NIBRS extract authorization and monitoring the extract process. The N-DEx PO enables the SDA capability within the N-DEx system.

1.6.4.4 Automated Processing Administrator (APA) – Responsible for activating, configuring, and managing the N-DEx optional automated processing capability. Automated processing enables an agency to receive reports reflecting correlations between their submissions and current N-DEx information.

1.6.4.5 Training Administrator (TA) – Responsible for managing the optional N-DEx Training function. This function includes the ability to maintain training logs

and generate reports as needed. The agency's CSA shall have the capability to utilize the training functionality for all agencies under its authority.

1.7 System Security

1.7.1 The CSA is responsible for establishing and administering an information technology security program throughout the CSA's user community consistent with roles and responsibilities described in the *Bylaws for the CJIS Advisory Policy Board and Working Groups* and the *CJIS Security Policy*.

1.7.2 The FBI uses hardware and software controls to help ensure system security. However, final responsibility for the maintenance of the security and confidentiality of CJI rests with the individual agencies participating in the N-DEx system. Further information regarding system security can be obtained from the *CJIS Security Policy*.

1.7.3 The data stored in the N-DEx system is documented CJI and must be protected to ensure authorized, legal, and efficient dissemination and use. It is incumbent upon an N-DEx participating agency to implement procedures to make the N-DEx system secure from any unauthorized use.

2.0 QUALITY CONTROL, VALIDATION, TRAINING, AND OTHER PROCEDURES

2.1 Maintaining System Integrity

2.1.1 Responsibility To Maintain System Integrity

2.1.1.1 Pursuant to the current version of the *Bylaws Of The Criminal Justice Information Services Advisory Policy Board And Working Groups,* the CSA is responsible for ensuring appropriate use, enforcing system discipline and security, and ensuring CJIS operating procedures are followed by all users, regardless of whether they are performed by CSA personnel, contracted support, an outside agency, etc.

2.1.1.2 A CSA may delegate responsibilities, including user management, to the NAC of subordinate agencies as outlined in the CJIS Security Policy.

2.1.1.3 The CSA may require notification of all new users given N-DEx through delegated user management. It is the CSA's responsibility to coordinate this notification process and the frequency of notification with the delegated "user management designee". This process will ensure the CSA has the desired level of involvement for user access since they remain ultimately responsible for all CJIS System of Services activities.

2.2 Security

2.2.1 Security standards are documented in the *CJIS Security Policy*.

2.3 Audit

2.3.1 Compliance audit: Compliance audit standards are documented in the *CJIS Security Policy*.

2.3.2 The FBI CJIS Division shall conduct compliance audits of CSAs that have agencies using the N-DEx system. Audits shall consist of the following:

2.3.2.1 Administrative interview with N-DEx local agency NAC.

2.3.2.2 Network inspection.

2.3.2.3 A review of random N-DEx transactions.

2.3.2.4 A review of user access.

2.3.2.5 Technical security and, if applicable, NCIC and III policies will also be assessed.

2.3.3 Audits will not include a review of data quality.

2.3.4 After one cycle of CSA informational audits, the FBI CJIS division shall incorporate the N-DEx audit into its existing audit cycle and audit findings will be provided to the APB for its review and appropriate action, which may include sanctions.

2.3.5 Security audits: Security audit standards are documented in the *CJIS Security Policy*.

2.3.6 Audits by the CSA: CSA audit responsibilities are documented in the *CJIS Security Policy* and Director approved APB guidance.

2.4 Training

2.4.1 CSAs may delegate N-DEx training to local agencies or regional information sharing entities.

2.4.2 Prior to searching data via N-DEx, CSAs shall ensure, directly or through local delegation, that users are trained on N-DEx policy matters, emphasizing data use rules.

2.4.3 Basic security awareness training shall be required within six months of initial assignment and biennially thereafter, for all personnel who have access to CJI.

2.4.4 Train N-DEx users granted access to leveraged CJIS System of Services system(s) in accordance with individual leveraged system training requirements.

2.4.5 Every two years, train users on N-DEx policy matters, emphasizing data use rules.

2.4.6 CSA shall ensure that all individuals with physical and logical access to N-DEx information are trained on N-DEx data use.

2.4.7 Maintain records of all training and proficiency affirmation.

2.4.8 The N-DEx PO shall make training materials available to the CSA. Training materials may take the form of any of the below:

2.4.8.1 Basic course hand out materials and curriculum.

2.4.8.2 Video training.

2.4.8.3 Computer based training modules.

2.5 Maintaining The Integrity of N-DEx Records

2.5.1 Record-owning agencies are responsible for the timeliness, accuracy, and completeness of their data. The records in the record-owning agency record/case management system are considered the source records.

2.5.2 Timeliness: Each record-owning agency shall submit data, including any updates or changes to the original submission as often as a contributor can feasibly execute them. Updates or changes shall be executed at least monthly.

2.5.3 Accuracy: Because records contributed to N-DEx will be limited to duplicates and summaries of records obtained and separately managed by the record-owning agency within its own record/case system(s), and for which the record-owning agency is responsible, each record-owning agency shall ensure contributed data is reflected within the source system(s). The record-owning agency shall ensure contributed data is synchronized with the Agencies source system records as they are updated/changed.

2.5.4 Completeness: Each record-owning agency should submit as many N-DEx data elements as they have available or are permitted to by law.

2.6 Quality Control

2.6.1 FBI personnel periodically check records entered into the N-DEx system. Issues discovered in records are communicated directly to the CSA and NAC.

2.7 N-DEx System Maintenance

2.7.1 When scheduled maintenance is being conducted on the N-DEx system, an information page will be displayed stating the expected outage time. If the N-DEx

system should become unavailable, outside of scheduled maintenance times, a warning banner will be displayed to the users. However, after a reasonable period of time and the problem is not resolved, notify the FBI CJIS, telephone 304-625-HELP [4357].

3.0 N-DEx SANCTIONS

3.1.1 In accordance with the *CJIS Security Policy*, each participating agency shall employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.

3.1.2 Upon any discovery of misuse by any users or agencies granted access to the N-DEx system, notification to their NAC and CSA must take place immediately.

3.1.3 Sanctions for misuse of N-DEx shall be established by the CJIS APB.

3.1.4 Sanctions for misuse of N-DEx-leveraged CJIS System of Services shall follow the established sanctions process for the CJIS System of Services.

3.1.5 Sanctions for *CJIS Security Policy* violations shall follow the established sanctions process.

APPENDIX A ACRONYMS

APA	Automated Processing Administrator
APB	Advisory Policy Board
CFR	Code of Federal Regulations
CHRI	Criminal History Record Information
CJI	Criminal Justice Information
CJIS	Criminal Justice Information Services
CSA	CJIS Systems Agency
CSO	CJIS Systems Officer
CUI	Controlled Unclassified Information
FBI	Federal Bureau of Investigation
IEPD	Information Exchange Package Documentation
III	Interstate Identification Index
LEA	Law Enforcement Agency
LES	Law Enforcement Sensitive
NAC	N-DEx Agency Coordinator
NCIC	National Crime Information Center
N-DEx	Law Enforcement National Data Exchange
PO	Program Office
POC	Point of Contact
SA	Security Administrator
SBU	Sensitive But Unclassified
SDA	Source Data Administrator
TA	Training Administrator
TAC	Terminal Agency Coordinator
UA	User Administrator

APPENDIX B APPROVED TECHNICAL & OPERATIONAL UPDATES

Through the CJIS Advisory Process, the following technical and operational changes have been approved or are awaiting approval of the FBI Director. Though a change may have been approved, changes do not become effective until implemented. All listed change is pending implementation.

FALL 2011 APB			
Title: Use Code			
APB ITEM #	PRIORTITY LEVEL	STATUS	IMPLEMENTATION DATE
5	NONE	PENDING Technical Enhancement	Spring 2013

Motion: Recommendation #1 (Continued): The APB moved to endorse the following policy statement for inclusion into the N-DEx Policy and Operating Manual. "Use Code: The FBI's CJIS Division maintains an audit trail of each disclosure and receipt of N-DEx data. Therefore, all N-DEx searches must include a Use Code identifying why the search was performed. The following Use Codes are considered acceptable when searching N-DEx:

i. Criminal Justice Use Code: Must be used when N-DEx is utilized for official duties in connection with the administration of criminal justice as the term is defined in 28 Code of Federal Regulations (CFR) § 20.3 (2011).

ii. Administrative Use Code: Must be used when N-DEx is utilized by a record-owning agency to retrieve and display N-DEx contributed records in association with performing the agency's data administration/management duty. Responses for this purpose shall not be disseminated for any other reason and are limited to the record-owning agency portion of N-DEx records.

While N-DEx supports this logging requirement through the N-DEx User Interface, entities accessing N-DEx data through a trusted broker must independently maintain these logs immediately and must automate the Use Code transmission prior to any additional use other than "c." ….

Technical Enhancement: YES

Policy Enhancement: Insert NEW POLICY: Use Code: The FBI's CJIS Division maintains an audit trail of each disclosure and receipt of N-DEx data. Therefore, all N-DEx searches must include a Use Code identifying why the search was performed. The following Use Codes are considered acceptable when searching N-DEx:

Criminal Justice Use Code "C": Must be used when N-DEx is utilized for official duties in connection with the administration of criminal justice as the term is defined in 28 Code of Federal Regulations (CFR) § 20.3 (2011).
. Administrative Use Code "A": Must be used when N-DEx is utilized by a record-owning agency to retrieve and display N-DEx contributed records in association with performing the agency's data administration/management duty. Responses for this purpose shall not be disseminated for any other reason and are limited to the record-owning agency portion of N-DEx records.

While N-DEx supports this logging requirement through the N-DEx User Interface, entities accessing N-DEx data through a trusted broker must independently maintain these logs immediately and must automate the Use Code transmission prior to any additional use other than "C."

FALL 2011 APB			
Title: Criminal Justice Employment Use Code			
APB ITEM #	PRIORTITY LEVEL	STATUS	IMPLEMENTATION DATE
5	NONE	PENDING Technical Enhancement	Spring 2013

Motion: Recommendation #2: The APB moved to endorse the recommended policy statement that addresses the privacy and legal concerns which have been previously identified by the Office of the General Counsel which reads: "The N-DEx Program Office will incorporate into the N-DEx Policy and Operating Manual the policies and language regarding Notice and Consent, Redress and Audits in order for the N-DEx system to be accessed for criminal justice employment background checks. "

Technical Enhancement: YES

Policy Enhancement: Insert NEW POLICY: as addition to NEW POLICY Use Code: "Criminal Justice Employment Use Code "J": Must be used when N-DEx is utilized to conduct criminal justice employment background checks or the screening of employees of other agencies over which the criminal justice agency maintains management control." Insert NEW POLICY: "Criminal Justice Employment Background Check Notice and Consent, Redress and Audit Requirements Insert NEW POLICY Notice and Consent: In order to use N-DEx to conduct criminal justice employment background checks, the agency must provide notice to the applicant and the applicant must provide a signed consent. At a minimum one of the following statements must appear on an agency's Notice and Consent form to an applicant:

General Statement:

The (agency's name)'s acquisition, retention, and sharing of information related to your employment application is generally authorized under (state and federal citations). The purpose for requesting this information is to conduct a complete background investigation pertaining to your fitness to serve as a (employee type). This background investigation may include inquiries pertaining to your (employment) (education) (medical history) (credit history) (criminal history) and any information relevant to your character and reputation. By signing this form, you are acknowledging that you have received notice and have provided consent for (agency's name) to use this information to conduct such a background investigation, which may include the searching of (N-DEx) (criminal justice databases) (private databases) (public databases).

Specific N-DEx statement:

I authorize any employee or representative of (agency's name) to search N-DEx to obtain information regarding my qualifications and fitness to serve as a (employee type). I understand that N-DEx is an electronic repository of information from federal, state, local, tribal, and regional criminal justice entities. This national information sharing system permits users to search and analyze data from the entire criminal justice cycle, including crime incident and investigation reports; arrest, booking, and incarceration reports; and probation and parole information. This release is executed with full knowledge, understanding, and consent that any information discovered in N-DEx may be used for the official purpose of conducting a complete employment background investigation. I also understand that any information found in N-DEx will not be disclosed to any other person or agency unless authorized and consistent with applicable law. I release (agency's name) from any liability or damage that may result from the use of information obtained from N-DEx.

Redress: In order to use N-DEx to conduct criminal justice employment background checks, the agency must provide applicants with an opportunity to challenge and/or correct records if

employment is denied based on information obtained from N-DEx. The task force agreed to the following redress process:

If employment is denied solely due to information obtained from N-DEx, and the applicant challenges the accuracy or completeness of those records, the denying agency shall provide the applicant with the contact information of the agency owning the information underlying the decision to deny. After receiving a written request from the applicant challenging the accuracy or completeness of the record used to deny employment, the record-owning agency shall then review the relevant information and advise the applicant in writing whether it has confirmed the accuracy or completeness of its records or whether the records will be corrected. If the applicant does not receive a response from the record-owning agency within 30 days from the date of the applicant's written request, the applicant may contact the FBI CJIS Division N-DEx Unit, 1000 Custer Hollow Rd, Clarksburg, WV 26306. The FBI shall forward the challenge to the record-owning agency for verification or correction. The record-owning agency shall then review the relevant information and advise the applicant in writing whether it has verified its records or whether the records will be corrected. Agencies should inform applicants of their responsibility to provide any corrected information to the denying agency that may assist the record owning agency in its research on behalf of the applicant.

Audit: In order to use N-DEx to conduct criminal justice employment background checks, the agency must comply with certain procedural and documentation requirements. The task force agreed to the following process:

All use of N-DEx for criminal justice employment background investigations shall require Use Code "J". Agencies that contribute records to N-DEx shall be permitted and enabled to reject Use Code "J" requests. When N-DEx is searched as part of a criminal justice employment background investigation, the fact that the search was conducted must be documented in the applicant's file. If information accessed through N-DEx is viewed and used during the criminal justice employment background investigation, the agency must document in the applicant's file: (1) that the requesting agency received advanced authorization for the use of the information for employment purposes from the record-owning agency and (2) that the requesting agency has confirmed the accuracy of the information with the record-owning agency.

Agencies are expected to comply with the above requirements in addition to the existing N-DEx policy requirements (e.g. training, information sharing, data quality, system security) and all applicable laws and regulations. These additional requirements mitigate the privacy risks of using N-DEx to conduct criminal justice employment background checks and ensure that such use is implemented in a lawful and proper manner.