DCJS Store and Forward Implementation Overview

Revised: November 2006

New York State Division of Criminal Justice Services
Office of Justice Information Services
Customer Service Group
4 Tower Place
Albany, New York 12204

DCJS Store
and Forward Implementation
Overview

I. Introduction to Store and Forward

In the traditional world of hardcopy inked fingerprint cards, New York State law enforcement agencies have been required to fingerprint arrested individuals multiple times to meet local, state, and federal requirements. Many enforcement agencies have to enter the same textual data on multiple cards as well.

Livescan and cardscan devices, however, permit an agency to acquire fingerprints only once and then use the acquired images for multiple reporting requirements. Agencies acquiring such equipment may transmit fingerprint images, along with other photo image and textual data, to DCJS electronically. This transmission process is known as Store and Forward.

The phrase 'Store and Forward' is often used in the field of electronic messaging to describe a methodology of routing information electronically from once location to another. In the criminal justice arena, it more narrowly addresses the transmission of data (biographic or pedigree data, such as name and address, sex, race, date of birth, etc. as well as related event-specific information), fingerprint images (as captured by use of a livescan device, which eliminates traditional ink-and-roll images, or by use of a cardscan device, a high resolution scanner which captures images from an inked fingerprint card), mugshots, palmprints, scars, marks, and tattoos, electronic signatures, and possibly other data pertinent to criminal justice processing. This information is then sent by a contributing agency to DCJS as an email (with attachment) over secure network lines or other approved connection method. Often this submission process traverses a county or regional server, which can store part or all of this information for later use at the local level. The formatting of messages must adhere to specifications and guidelines published by NIST (the National Institute of Standards and Technology, U.S. Commerce Dept.), the FBI, and DCJS. (*Please see section II.A below for more information on these specifications.*)

Once DCJS' processing is completed, information and images can be stored at the state level. Additionally, if the transaction qualifies for submission to the FBI, it will be forwarded electronically by DCJS so that the FBI's processing can also be accomplished within a short time frame. State and federal fingerprint-based responses are now typically available within a few hours of the initial submission to DCJS, and occasionally are both completed in less than an hour.

The 'Store and Forward' pilot project was implemented in November 1999 between DCJS and a consortium of eleven arresting agencies in Monroe County. The scope of the pilot project supported adult arrest, juvenile arrest, and criminal inquiry submissions. Messages contained both text and fingerprint image data, and could also contain mugshots and signatures. All fingerprint images acquired from either cardscan or livescan devices met the technical specifications set forth in DCJS' EBTS document and the '*Policy for Acquisition and Implementation of Livescan, Cardscan and Photo Imaging Systems*.'

The pilot phase was developed at DCJS as part of the National Criminal History Improvement project and was managed by the DCJS Advanced Technology Group with assistance from Comnetix Computer Systems, Inc. It relied on manual processes at DCJS

to transfer this data into the computerized criminal history (CCH) database and to trigger sending identification responses back to the contributor.

The next phase was implemented in March 2000, and concentrated on improvements and enhancements needed to allow for expansion of the contributor base to Store and Forward. DCJS' development of a 'Store and Forward manager' streamlined processing for message control and data entry.

Subsequent and significant developments have continued, including the ability to submit qualifying transactions directly to the FBI electronically, and providing for the submission of civil, jail admission, probation/parole supervision, dead prints, sex offender, FBI criminal resubmission, and FBI civil resubmission transactions. Additionally, DCJS plans to provide a fully functional image search and retrieval system for mugshots (including line-up capability) and scars, marks, and tattoos.

II. Pre-Implementation Issues

Agencies desiring to implement a Store and Forward system will need to address many issues beyond the simple acquisition of livescan or cardscan hardware. The introduction of this technology impacts many local processes. In addition, there are technical concerns to resolve in order to effectively and securely communicate with DCJS.

This document will briefly describe these tasks in order to provide an overview and working checklist for agencies wanting to implement store and forward systems. This overview is by no means comprehensive, and it is only intended to foster discussions within agencies at the local level as well as with DCJS.

A. Design and Policy Impacts

The primary design document for sites pursuing store and forward technologies is the *New York State Criminal Justice Electronic Biometric Transmission Standard* (NYSCJEBTS, or more commonly, EBTS). Store and Forward sites will be required to adhere to the standards described in the EBTS. The initial version was published in February 1998. Anyone desiring to view or print the latest version can find it at http://criminaljustice.ny.gov/advtech/ebts.pdf

Agencies implementing Store and Forward may also need to work with DCJS to update their Use and Dissemination (U&D) agreements, if such agreements are not current and up-to-date. (*See item II.A.2 below*.)

1. EBTS Requirements

As mentioned above, the EBTS is the acronym for the *Electronic Biometric Transmission Standard*. Contributors wishing to submit electronic transactions to DCJS must adhere to this standard.

The FBI's *Electronic Biometric Transmission Specification* (IAFIS-DOC-01078-7.1) contains background information on why such a standard exists. The FBI and the National Institute of Standards and Technology (NIST), along with advice from others in the criminal justice community, have developed a standard for electronically encoding and transmitting fingerprint image, identification, and arrest data. This EBTS references additional standards developed by the American National Standards Institute (ANSI) entitled 'American National Standard for Information Systems - Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information' (ANSI/NIST-ITL 1-2000). This defines the content, format, and units of measurement for the exchange of information that may be used in fingerprint identification. The use of such standards facilitates the interchange of such data between various criminal justice organizations, and provides a common format so that systems from various vendors can easily share such information.

In summary, the NIST-defined format for data and image transmission is currently based on utilization of numbered tags (or record identifiers) within specified record types. A "Type 1" record, for instance, is basically a header record used between systems to identify a transaction; "Type 2" records contains descriptive and biographical date; "Type 4" records contain fingerprint images; "Type 8" records contain signatures; and "Type 10" records contain photographs. (There are other record types in addition to these.)

When a transaction is received by DCJS, a software program deconstructs the message and stores the individual data items in an Oracle database. When transmitting to another agency, the database fields are built into a new NIST-format compliant record and sent.

In addition to this 'traditional' numeric tagged format, NIST plans to issue an XML version of this specification sometime in 2006 or 2007.

DCJS recognized the need for additional tags and policies (beyond those defined by the FBI) to govern transactions between agencies within the State of New York. As a result, DCJS issued its own version of the EBTS in 1998, entitled *New York State Criminal Justice Electronic Biometric Transmission Standard.* This document continues to evolve as business needs and market changes dictate. Its purpose is to further specify the requirements to which agencies must adhere in order to electronically submit certain types of processing requests to DCJS, and it defines the inclusion of additional data not found in the federal standard. These requirements include the specifications to be employed, transmission protocols to be followed, and the format and content of the messages transmitted.

It should be noted that as the ANSI/NIST and DCJS specifications continue to mature and be updated, every effort will be made to minimize the impact on software developed prior to such changes. Any further changes to the data

fields or formats for these submissions should not cause invalidation of existing systems in place at user agencies. For example, if a change to a field definition results in a new tag being assigned reflecting the new definition, the old tag will remain acceptable for the original definition. Additional fields will simply be given a tag number as the need arises. In this manner, each user agency has the opportunity to enhance its own system to take advantage of the change(s) on its own schedule.

The present release of the NYSCJEBTS details electronic submissions in lieu of physical fingerprint cards and mugshot/photo submissions. Later releases may add additional functionality such as latent and/or palm print submissions, requests for archived fingerprint and/or photo images, the updating of biographic or event information, submission of new photos, etc.

2. Use and Dissemination Agreements

Pursuant to New York State Executive Law §837(6) and §837(8), the Division of Criminal Justice Services (DCJS) is the State repository for Criminal History Record Information (CHRI) and other data, and requires DCJS to assure the security and privacy of this data. Access to CHRI is limited to authorized criminal justice agencies as defined in Executive Law §835(9), and the agencies authorized by law to conduct criminal history background checks for employment and licensing purposes. DCJS requires all CHRI user agencies to have an executed "Use and Dissemination Agreement" (U&D) on file. This U&D outlines the terms and conditions of CHRI access, services to be provided, and permissible use of the information obtained.

Execution of a U&D requires that a user agency abide by State and Federal administrative regulations, policies and laws regarding the use and exchange of criminal history, wanted, and missing persons data. Agency personnel should be aware of the U&D's provisions, especially the requirement to maintain supporting documentation to facilitate audits, allowable reasons for making an inquiry, and dissemination of data. A comprehensive explanation of all applicable statutes and regulations is contained within the U&D. *Access to CHRI will not be available to an agency until the U&D is executed by both parties.*

Note: If an authorized agency has a U&D executed with DCJS subsequent to April 1999, there is no need to re-execute a new U&D for transactions to be submitted via Store and Forward.

B. Local Process Impacts

1. For Arresting Agencies: Booking Process and Court Information Flow

Perhaps the most readily apparent impact that the installation of a livescan or cardscan device will have is on the booking process that takes place at a local

arresting agency. When a system for collecting booking data (such as a Records Management System, or RMS) already exists, the agency will want to work with its vendors to integrate the flow of data and images between the various components of the system.

A secondary impact of a store and forward implementation is the more rapid availability of identification results (as verified by fingerprint comparisons) from the state and federal levels. Whereas identification results may not previously have been delivered in a timely fashion, Store and Forward provides an extremely fast identification result turnaround time from time of fingerprint transmission to the state. As mentioned previously, the DCJS goal for arrest and inquiry submissions is to respond within three hours and the FBI within two hours, but the average turn-around time is usually substantially less than that. As a result, agencies may want to factor the ready access to fingerprint-confirmed warrant and prior criminal history information into their local decision-making processes – that is, they may choose <u>not</u> to prematurely release on bail or recognizance those individuals not already known to them, so as to provide time for both state and federal responses and a positive identification.

Less apparent is the impact of Store and Forward on the flow of information to the courts and district attorneys. In any arrest, there is information which must be supplied to the court, including an updated rapsheet and the criminal justice tracking number (CJTN, formerly known as the Court Control Number or OBTS Number). In an environment where paper fingerprint cards are used, this tracking number is reported to the courts via the perforated stub from the arrest fingerprint card and the rapsheet is delivered in any one of a number of options: mail, as a secondary copy delivered to the police department, etc.

With Store and Forward, the CJTN is centrally assigned by DCJS and is returned along with the acknowledgment of the fingerprint transmission. Because utilization of a livescan machine (or cardscan, if using other than a DCJS preprinted arrest card as a capture document) eliminates the availability of the stub with preprinted CJTN number on it, care must be taken to provide the court with the correct CJTN supplied by DCJS. Ideally, this would happen when the court receives the rapsheet containing the appropriate arrest and CJTN. In some circumstances, other alternatives may have to be worked out with your vendor and the courts (such as printing some sort of court document with the CJTN and other pertinent information).

Agencies implementing Store and Forward should recognize that rapsheets can now be delivered in time to make arraignment decisions. Localities may want to give some thought to encouraging their local court and district attorney to have access to eJusticeNY, so that *all* agencies can be provided electronic raps immediately after DCJS and FBI processing is complete. A more thorough discussion of rapsheet options is provided later in this document.

2. For Other Criminal Justice Agencies

Courts may submit fingerprint-based criminal inquiry transactions to DCJS in order to determine or verify an individual's identity. The advantage to a court is that the very latest rap information is then provided, and it is absolutely linked to an individual by fingerprints. This may also be desirable when the original arrest prints submitted to DCJS by the arresting agency were of poor quality, and the court subsequently orders a new set of prints to be taken and submitted to better confirm actual identity.

In a corrections environment, fingerprint-based inquiry transactions can also provide this same service, permitting classification of individuals being held at the facility. DCJS can also accept 'admission' transactions for those individuals sentenced to time in a county facility (if the top charge is 'fingerprintable' based on state law and/or when the sentence is for more than 15 days), or when sentenced to a year or more at a state facility.

Supervisory agencies (parole and probation departments) can also notify DCJS of the status of someone now in their custody, and the criminal history of such individuals will be updated accordingly. This also permits subsequent notification to the supervisory agency if their subject is later arrested.

3. Civil Agencies

Using Store and Forward permits contributors of civil fingerprint transactions to greatly reduce the overall processing time of an individual who is applying for employment, permit, license, or clearance whenever a fingerprint-based background search is required. In the ink-and-roll world, cards would be mailed to DCJS, processed, and then any resulting rap sheets would be mailed back to the contributor. The turn-around time, which often took several weeks (especially if an FBI search was also required), has now been tremendously reduced. Our current goal for electronically received civil fingerprint transactions is to respond with a new or updated rap sheet within two days of initial receipt of a transaction, though this end-to-end processing time is often less than that.

4. Standard Practices for Criminal Cases

Because of the introduction of livescan and cardscan technologies and the accompanying changes, localities have the opportunities to make system improvements by implementing the practices set forth in the on-going Standard Practices project. The goals of the project have been to develop practices and procedures designed to collect data correctly and efficiently and to promote the smooth exchange of information among all agencies and jurisdictions involved in the criminal justice process.

The development and dissemination of a compendium of Standard Practices has been a critical step toward establishing a foundation for the improvement of criminal history data quality in New York State. These practices will involve an on-going cycle of training, monitoring and updating of standards.

The implementation of any new technology, but especially livescan and cardscan, should include a review of current business practices. Furthermore, analysis should focus on possible improvements that can be made as a result of the introduction of new systems. Every criminal justice agency should already have a copy of the 'New York State Standard Practices for Processing Fingerprintable Criminal Cases,' published by DCJS in September 2001. This document may be order from DCJS by calling the Customer Contact Center at 1-800-262-3257, or by accessing the DCJS public website at http://criminaljustice.state.ny.us/stdpractices/main_menu.htm. The 'Arrest Processing' section describes methods for collecting and reporting data to DCJS which should be incorporated into the Store and Forward interface and into the business processes of the local agencies. There is also a helpful section for 'Custody and Supervision Processing.' Where questions or difficulties arise with adopting any of the Standard Practices, DCJS is available to work with individual sites.

C. Networking

To ensure the proper routing of livescan and cardscan transactions between the DCJS system and contributing agencies, certain network requirements must be met. Livescan and cardscan transactions ***cannot*** currently be routed over the internet directly to DCJS, though internet connectivity with added VPN security can be used between a host county (regional) server and their end-user community. For larger sites, DCJS supports MQSeries, and smaller sites can still use SMTP for data transfer (most of the following applies to SMTP connections).

1. IP Addresses

All routing on TCP/IP networks is based on unique IP network addresses. The IP addresses used for the Livescan/Cardscan systems must not be accessible via the Internet. If an address is accessible over the Internet or it is not unique, routing problems can occur and the messages may be routed over the Internet or to the wrong mail server.

Either **a** or **b** is required:

a. IP Addresses must be registered by the contributing agency with the American Registry for Internet Numbers (ARIN) and not propagated on the Internet. For further information on address registration, please see the ARIN website at www.arin.net.

b. IP Addresses must be registered with the NYS Office for Technology - Network Coordinating Unit. The OFT NCU maintains a private class A 10 address space. Any government agency that uses the NYeNet, or connects to an agency that uses the NYeNet, can obtain an IP network address from the OFT NCU. For further information or to request an address space, please contact the NCU through the Customer Contact Center of DCJS at 1-800-262-3257.

2. Domain Name Services

Domain Name Services associate an IP address with a domain name. In most cases, DCJS will assign the domain name for a given customer, since this name is never used on the public internet and is solely used within an isolated system. Networking staff at DCJS can assist with any questions.

3. Physical Connection

Each customer is responsible for acquiring and maintaining the appropriate communication equipment to establish a network connection to DCJS. Customers looking to establish such a connection must contact Infrastructure Support through the Customer Contact Center of DCJS at 1-800-262-3257. Users will need to provide the following information:

a. Name and phone number of site's network coordinator
b. Location and type of network equipment
c. Number of anticipated of livescan/cardscan devices that will be used

Based on the supplied information and an interview with the network coordinator, DCJS staff will assist the customer in setting up the initial physical connection into DCJS' network. This assistance could range from help in ordering circuits, CSU/DSUs, and routers to configuration and testing. DCJS will provide the customer with a network diagram of the planned physical connection which will be used for future troubleshooting purposes. Ultimately the customer will be responsible for all support and maintenance of their equipment including whatever equipment is used for the physical connection. Use of the NYeNet is highly recommended for all governmental agencies, though direct line connections might be required in other cases.

4. Security

In order to secure the traffic between networks, DCJS and the customer will need to exchange appropriate IP addresses for servers at each site. On the DCJS side, all livescan or cardscan traffic will pass through a firewall; therefore only devices which are known to DCJS will be allowed to pass. If one or more firewalls exist within the customers' network that would be involved with livescan /cardscan transactions, the user will need to make the appropriate updates to their own firewall.

5. Routing Information

DCJS and the customer may need to exchange additional routing information as appropriate. DCJS does not support any routing protocol into/out of any other organization's network.

6. Network Monitoring

DCJS requests that certain network monitoring devices within its network be allowed ICMP access to the livescan/cardscan devices. This is for troubleshooting and normal network purposes and is a negotiable item. DCJS will consider the same type of request for user's network management.

III. System Installation and Implementation

A. Testing Requirements

Most contributors who wish to submit electronic transactions to DCJS (using either livescan and/or cardscan fingerprint image capture technology) will need to conduct a formalized test with DCJS. This is always true for the first agency using a new central or regional server. (A more limited test is often used for a new user submitting through an already-operational server.) All civil sites and central criminal sites will need to need to complete a checklist for DCJS, as well as conducting a scripted test. The purpose of this formal test is:

- To ensure EBTS compliance (both on the messaging level and on the individual field level)
- To make sure all communications protocols and connections work properly
- To make certain that fingerprint images submitted to DCJS are of a high enough quality to be used when searching against our SAFIS database

DCJS has established a basic test suite which needs to be run before any new server site can be considered for acceptance into a live production environment. The results of this test need careful review by DCJS staff, and if necessary, certain tests may need to be rerun after appropriate software or hardware changes are made. For criminal arrest agencies, the kinds of tests are:

- Arrest submissions (adult and possibly JD)
- Inquiry submissions
- Incarceration submissions
- Supervision submissions
- Sex offender registry submissions
- Resubmission of DCJS rejects for either image or data problems
- Resubmission of FBI rejects for either image or data problems
- Graceful handling of various kinds of component outages and/or interruptions

- Response generation - Transactions will receive either a positive identification response, a non-ident response, error rejects for image /and or data problems, or no response at all (which tests the contributor's internal reporting mechanism)

Civil agencies and inquiry-only agencies (such as courts) will have a similarly designed test with transactions pertinent to their usual business process.

DCJS reserves the right to add, modify, or delete tests as conditions, experience, and further enhancements dictate. Contributors can also arrange for specific tests, if requested, to test local system behavior.

Contributors should plan on testing lasting a minimum of ore or two days, although longer testing periods may be required if significant difficulties arise. The Quality Assurance Group at DCJS will be the main contact for coordination of testing, establishment of dates, and the conducting of any tests. You may contact Quality Assurance staff through the Customer Contact Center of DCJS at 1-800-262-3257, and request the assistance of the 'Store and Forward Implementation Team.' Due to the intensive nature of testing and the necessity of having dedicated test resources available at DCJS, such testing needs to be run consecutively (that is, DCJS cannot normally test with more than one contributor at a time).

B. Implementation Schedule

DCJS will ask each local agency to request a testing window (or test slot) when ready to test with DCJS. It is expected that if testing results are satisfactory and acceptable to DCJS, an agency should be able to go 'live' immediately or within a few weeks at most from the completion of testing.

If a site is unable to test during its assigned period or if the test results are not acceptable, the site will be given a new testing period based on the availability of DCJS and the local agency resources.

If a site has a protracted period of more than a few weeks between test completion and being able to go live, then some retesting may need to be done, as DCJS' discretion.

C. Operational Support

The DCJS Office of Identification and Special Services ('Operations') is responsible for day to day processing of arrest fingerprint transactions. In this capacity, Operations interacts with contributing agencies to ensure that their fingerprint transactions meet DCJS' image and data quality standards for successful identification processing. The identification process results in the production of the New York State Criminal History Record.

In order for Operations support to work effectively, several areas of mutual concern need to be addressed and discussed to insure a successful livescan implementation. These areas include, but are not limited to 24 hour (contributor) contact names and phone numbers, understanding of re-roll options, poor print processing options and effects, arraignment strategies and priority processing, inquiry versus arrest transaction processing, single versus multiple agency submissions, livescan/cardscan options, livescan fall back plan, and contributor maintenance support.

Once operational, problems with specific transactions can be addressed to the Customer Contact Center at 1-800-262-3257. They will forward your call to the appropriate DCJS Operations staff for assistance. You can also utilize the 'Feedback' option in eJusticeNY to get assistance.

IV. Rapsheet Delivery Options

One of the primary products of a Store and Forward submission to DCJS is the creation of a new or updated criminal history report, or rapsheet. As part of the analysis for implementing Store and Forward, local agencies will need to evaluate their current mechanisms for receiving rapsheets. These agencies will need to work with DCJS to ensure their Store and Forward transmissions are handled properly and the rapsheet is routed to the correct destination.

EJusticeNY is the primary mechanism currently used for returning rapsheets and subsequent hit notices, using the agency's civil and/or criminal in-box. Any unique local needs should be discussed with DCJS prior to moving into full scale operation. DCJS also encourages agencies to coordinate rap distribution, when required, with the courts and/or District Attorneys. EJusticeNY is available to these agencies as well, and many are already using it. Any agency not currently using eJusticeNY should request enrollment information from the Customer Contact Center at 1-800-262-3257.

Use of Fax Prefixes

A few criminal sites currently using fax equipment have a unique fax prefix. Some agencies have their raps routed based on the fax prefix or have internal / local processing needs which require a continuation of fax numbers. DCJS wants to discontinue the use of fax equipment and fax numbers as agencies move to Store and Forward, and will work with agencies if they feel there is a critical business need to continue using such a fax prefix. If you do not currently use fax equipment, this item does not pertain to you.

Agencies should be aware the use of fax prefixes will eventually be phased out by DCJS, as fax equipment is old, and difficult and expensive to maintain.

<u>EJusticeNY Rapsheet</u>

***Background*:**

What is it? EJusticeNY is a secure extranet site, accessed with a standard browser, developed to meet the needs of the Criminal Justice community. Many distinct service suites are currently available, and more are being added constantly. Most agencies have some or all of the available suites, as their needs dictate.

Who gets it? Generally speaking, any authorized individual from an agency that has a legal right to CCH information can get access. More specifically, an authorized agency must complete an application which includes a new Use and Dissemination (U&D) Agreement and must specify the individuals for whom access is being requested. Each agency must designate a Terminal Access Coordinator (TAC) for eJusticeNY so that DCJS can be informed of changes of operators and tasks permitted each one.

Availability: EJusticeNY is now available for all agencies which complete the application and U&D process. To request enrollment information and an application, please call the DCJS Customer Contact Center at 1-800-262-3257.

Other requirements: The information can be accessed using a personal computer (PC) via a dial-up phone line or from a networked PC. Other than connectivity, the only software requirement for the end-user is a commercially available web-browser such as Microsoft Internet Explorer.

Behind the Scenes:

Suppression: Based on the individual's logon and the stated reason for request, a database is consulted which tracks the associated agency's U&D agreement and determines whether the request is valid and also controls the appropriate level of data to release. This process occurs for both the Inquiry and Search Services.

Logging: All inquiry and search requests and resulting disseminations are logged and can be accessed by DCJS Audit staff.