

AUDIT REPORT



CITY OF NEW YORK
OFFICE OF THE COMPTROLLER
BUREAU OF FINANCIAL AUDIT
WILLIAM C. THOMPSON, JR., COMPTROLLER

Audit Report on the Development and Implementation Of the Department of Investigation Livescan Fingerprint System

7A04-067

April 6, 2004



THE CITY OF NEW YORK
OFFICE OF THE COMPTROLLER
1 CENTRE STREET
NEW YORK, N.Y. 10007-2341

WILLIAM C. THOMPSON, JR.
COMPTROLLER

To the Citizens of the City of New York

Ladies and Gentlemen:

In accordance with the responsibilities of the Comptroller contained in Chapter 5, § 93, of the New York City Charter, my office has performed an audit of the development and implementation of the Department of Investigation Livescan Fingerprint System. The results of our audit, which are presented in this report, have been discussed with officials of the Department of Investigation, and their comments have been considered in preparing this report.

Audits such as this provide a means of ensuring that City agencies are developing computer systems in an efficient, timely, and cost-effective manner.

I trust that this report contains information that is of interest to you. If you have any questions concerning this report, please contact my Audit Bureau at 212-669-3747 or e-mail us at audit@Comptroller.nyc.gov.

Very truly yours,

A handwritten signature in cursive script that reads 'William C. Thompson, Jr.'.

William C. Thompson, Jr.
WCT/gr

Report: **7A04-067**
Filed: **April 6, 2004**

Table of Contents

AUDIT REPORT IN BRIEF	1
INTRODUCTION	3
Background	3
Objectives	4
Scope and Methodology	4
Discussion of Audit Results	5
FINDINGS AND RECOMMENDATIONS	6
The Cardscan Subsystem Is Not Operational	6
System-Development Methodology	6
Disaster Recovery Plan Is Not Complete	7
User Satisfaction	7
Other Issues	7
Recommendations	8
ADDENDUM DOI Response	

*The City of New York
Office of the Comptroller
Bureau of Financial Audit
EDP Audit Division*

**Audit Report on the
Development and Implementation of the
Department of Investigation
Livescan Fingerprint System**

7A04-067

AUDIT REPORT IN BRIEF

We performed an audit on the development and implementation of Livescan, an automated fingerprinting system, by the Department of Investigation (DOI). Livescan captures and transmits fingerprint images electronically. The system significantly reduces the turnaround time for fingerprint checks and eliminates the need to resubmit to the State fingerprints that have been rejected because of poor image quality.

Audit Findings and Conclusions

Livescan meets DOI's initial business and system requirements for capacity to transmit information to and receive information from the New York State Division of Criminal Justice Services (DCJS). According to our user survey, users of Livescan are generally satisfied with the system because it reduces turnaround time. Further, the system allows for future changes and periodic upgrades. In addition, DOI complied with the applicable New York City Procurement Policy Board (PPB) rules when procuring the system. However, although DOI stated that it had implemented all of the four system components included in the original contract, it could not demonstrate that the Cardscan subsystem is operational. Moreover, DOI did not follow a system-development life-cycle methodology, nor did it provide for an independent quality-assurance test of the system. Therefore, we could not determine whether Livescan would, as a finished product, meet the overall goals as stated in the system justification. Also, although DOI has included Livescan in its disaster recovery plan, the plan is not complete.

During fieldwork, we noted that: DOI does not ensure that passwords for the Livescan and the DCJS computer system (Secure Services) are periodically changed; the system firewall security is below DOI standards; security policies are not up-to-date; and DOI does not adequately monitor security violations. In addition, DOI lacks an adequate fire suppression system to protect Livescan. Finally, DOI did not ensure that it has access to the Livescan source code in the event

that the vendor, Comnetix Computer Systems (Comnetix), goes out of business or is otherwise unavailable and programming changes are required.

Audit Recommendations

To address these issues, we recommend that DOI:

- Ensure that the Cardscan subsystem is operational and that appropriate personnel are trained in its operation.
- Follow a formal systems-development methodology for all future systems-development projects and engage an independent quality assurance consultant or assign an employee to monitor and review development work, as well as any system enhancements to Livescan. In addition, DOI should develop formal acceptance-sign-off procedures to ensure that all system requirements are completed.
- Develop procedures to determine whether an event is sufficiently serious to invoke its disaster recovery plan. In addition, DOI should formalize agreements with the vendors to provide software supplies and equipment and with DoITT regarding the alternate processing site. Finally, DOI should periodically test the disaster recovery plan.
- Address the user concerns revealed in our survey. In that regard, DOI should consider including help menus and screens and formats that are easier to use and providing additional training to those users who reported that they had limited knowledge of the system.
- Ensure that its employees periodically change their passwords for Livescan and Secure Services.
- Upgrade its CISCO PIX firewall version to the standards set by its CISAFE (Citywide Information Security Architecture Formulation and Enforcement) unit.
- Establish formal procedures to document and report system-access violations, and review and follow up on all reported violations. In addition, DOI should ensure that maintenance of security documentation is accurate and complete.
- Install a fire-suppression system that would protect the equipment. In addition, DOI should document the fire prevention procedures in effect at its Chambers Street facility.
- Obtain the Livescan source code in case the vendor should become unavailable.

INTRODUCTION

Background

DOI assures integrity in City government through investigations and studies initiated by the Mayor, the City Council, or the DOI Commissioner, or in response to complaints from the general public and City employees. The Inspectors General and investigative staff of DOI conduct criminal investigations into allegations of corruption and fraud perpetrated by City employees, contractors doing business with the City, and people receiving benefits from the City. DOI staff also analyzes and studies various aspects of City government to identify management practices, operations, and programs in need of improvement, and to recommend strategies that will help agencies limit opportunity for criminal misconduct and waste.

Prior to May 24, 2002, DOI performed background checks of existing and prospective City employees as well as those of City-licensed programs, such as child-care, home care, and family shelter programs, by fingerprinting individuals and sending the prints to DCJS. The background-check process took some time to complete; it entailed taking fingerprints manually, mailing the fingerprint cards to DCJS through the U.S. Postal Service, and then, after the cards had arrived at DCJS, waiting four to six weeks to receive the results.

On May 24, 2002, DOI implemented an automated fingerprinting system known as Livescan. The Livescan system, which has been implemented at DOI and at Police Department precincts throughout the City, captures and transmits fingerprint images electronically. The system significantly reduces the turnaround time for fingerprint checks and eliminates the need to resubmit fingerprints that have been rejected because of poor image quality.

Livescan was procured through a New York State Office of General Services requirements contract in accordance with the PPB rules. DOI selected Comnetix to provide the system and five years of maintenance at a cost of \$199,400. Specifically, Comnetix was to provide a system consisting of the following components:

- Livescan Fingerprint Subsystem: Software and hardware equipment to record fingerprints. The fingerprint images were to be compressed using a FBI-approved compression algorithm.
- Cardscan Subsystem: Software and hardware that enables users to print copies of fingerprint images. This subsystem is intended as a backup to the Livescan subsystem component.
- Integration Module Equipment: Enables equipment to transmit fingerprints to and receive responses from DCJS in accordance with the New York State Criminal Justice Electronic Fingerprint Transmission Standards.

- The Integrated System: Ensures that the above components interface with each other and that the system complies with the New York State Criminal Justice Electronic Component Interface Standards.

Objectives

The audit objectives were to determine whether:

- Livescan meets DOI's initial business and system requirements;
- The system design allows for future enhancements and upgrades;
- Livescan, as a finished product, will meet overall goals as stated in the system justification;
- Livescan was procured in compliance with PPB rules;
- DOI followed a formal system-development methodology when developing Livescan; and,
- Livescan has been incorporated into DOI's disaster recovery plan.

Scope and Methodology

Our fieldwork was conducted from September 2003 through December 2003. To achieve our audit objectives, we interviewed DOI officials and:

- (1) Reviewed specification documents, contracts, purchase orders, and other system-related documentation;
- (2) Conducted a system walk-through;
- (3) Tracked system transactions to test whether the system performed as intended;
- (4) Reviewed DOI's records concerning rejected fingerprint-check transactions to determine whether Livescan decreased the incidence of such rejections; and
- (5) Tested compliance to all applicable PPB procurement criteria including provisions for using state requirements contracts.

In addition, we conducted a satisfaction survey of DOI's 14 Livescan users (all of whom responded) and four employees in City agencies who act as contacts for the licensed programs (three of the four individuals responded; the individual who did not respond is an ACS employee). The general purpose of the survey was to determine whether users are satisfied with the system,

whether they have been appropriately trained, and what changes they would like made to the system.

We used Comptroller's Internal Control and Accountability Directive 18, *Guidelines for the Management, Protection and Control of Agency Information and Information Processing Systems*, all relevant sections of the PPB rules, and DOI's Citywide Information Security Architecture Formulation and Enforcement (CISAFE) standard. Since the City has no formal system-development methodology, we used the National Institute of Standards and Technology Special Publication 500-233, *A Framework for the Development and Assurance of High Integrity Software*, to assess whether DOI had followed a formal methodology.

This audit was conducted in accordance with generally accepted government auditing standards (GAGAS) and included tests of the records and other auditing procedures considered necessary. This audit was performed in accordance with the audit responsibilities of the City Comptroller, as set forth in Chapter 5, § 93, of the New York City Charter.

Discussion of Audit Results

The matters covered in this report were discussed with DOI officials during and at the conclusion of this audit. A preliminary draft was sent to DOI officials and discussed at an exit conference held on February 23, 2004. On March 5, 2004, we submitted a draft report to DOI officials with a request for comments. We received a written response from DOI officials on March 19, 2004. In their response, DOI officials agreed with the six of the nine recommendations and partially agreed with the three remaining recommendations, but disagreed with the corresponding findings, namely that: DOI did not demonstrate that the Cardscan subsystem is operational; did not follow a formal system-development methodology; and did not develop a complete disaster recovery plan.

The full text of the DOI response is included as an addendum to this report.

FINDINGS AND RECOMMENDATIONS

Livescan meets DOI's initial business and system requirements for capacity to transmit information to and receive information from DCJS and according to our survey, users are generally satisfied with the system because it reduces turnaround time. Further, the system allows for future changes and periodic upgrades. In addition, DOI complied with the applicable PPB rules when procuring the system. However, although DOI stated that it had implemented all of the four system components included in the original contract, it could not demonstrate that the Cardscan subsystem is operational. Moreover, DOI did not follow a system-development life-cycle methodology, nor did it provide for an independent quality-assurance test of the system. Therefore, we could not determine whether Livescan would, as a finished product, meet the overall goals as stated in the system justification. Also, although DOI has included Livescan in its disaster recovery plan, the plan is not complete.

During fieldwork, we noted that: DOI does not ensure that passwords for the Livescan and the DCJS computer system (Secure Services) are periodically changed; the system firewall security is below DOI standards; security policies are not up to date; and DOI does not adequately monitor security violations. In addition, DOI lacks an adequate fire suppression system to protect Livescan. Finally, DOI did not ensure that it has access to the Livescan source code in the event that Comnetix goes out of business or is otherwise unavailable and programming changes are required.

These issues are discussed in the following sections of the report.

The Cardscan Subsystem Is Not Operational

As indicated previously, there were four components to the Livescan project. One of these components, the Cardscan subsystem, was intended as a backup to the Livescan Subsystem if transmission problems arose between Livescan and DCJS. According to DOI officials, Cardscan was developed and installed; however, they were unable to demonstrate the operation of the Cardscan system to us. Therefore, we could not verify DOI's assertion that Cardscan is installed and operational or determine whether it functions as intended.

System-Development Methodology

DOI did not employ a formal system-development methodology when it developed Livescan. Comptroller's Directive 18, § 9.5.1, states that following "a formal system development methodology to manage the development process" can help "insure the success of system development projects." In addition, DOI officials stated that the Livescan modules needed for data transmission between Livescan and DCJS were successfully tested. However, DOI did not maintain the test scripts, final testing results, or acceptance certificates for Livescan. Therefore, we cannot determine whether all the system tasks and requirements were thoroughly tested and completed. Furthermore, we attribute the inability of DOI to demonstrate that Cardscan is operational and its failure to maintain testing documentation to its not having an individual to independently provide

quality assurance to the project. Directive 18, § 9.5.1 recommends that for critical projects, agencies use an independent quality assurance individual to assist the agency in monitoring and reviewing the work of the development team. Such an individual would have ensured that applications, systems, and programs were developed and implemented in accordance with DOI intentions.

Disaster Recovery Plan Is Not Complete

Although our review revealed that DOI included Livescan in its disaster recovery plan, we found that the plan, as a whole, is incomplete. Specifically, DOI's Technology Division developed an outline of the applications that would be restored should a disaster occur, a contact list of personnel critical to continuing system operation, and an alternate processing site at the Department of Information Technology and Telecommunications (DoITT) to be used in case of a disaster at DOI. However, DOI's plan does not include: procedures to determine whether an event is sufficiently serious to invoke the plan, a formal agreement with vendors to provide software supplies and equipment, a formal agreement with DoITT for the alternate processing site, and procedures for manual processing and testing.

User Satisfaction

Our user-satisfaction survey revealed that system users are generally satisfied with its operation. However, seven of 14 DOI users indicated that they would like to see minor changes made in Livescan. These changes include help menus, and screens and formats that are easier to use. In addition, Comnetix generally provided a half-day of training on the system's operations. Three DOI employees who received this half-day of training stated that they felt their knowledge of the system was limited because of poor training.

Other Issues

During fieldwork, we noted that DOI employees are not required to change their passwords periodically when logging on to Livescan and to the DCJS computer system, Secure Services. Livescan requests information on fingerprints taken by DOI from Secure Services, which stores records of arrests and convictions from the State and the federal government. Directive 18, § 8.1.2, states that "active password management includes insuring that users are forced to change passwords periodically." Periodic password changes provide an additional layer of security to ensure that only authorized users access the systems.

In addition, although DOI uses the CISCO PIX firewall to protect the internal network from the external network, the version used does not meet the standards set by its CISAFE unit. The higher version would allow DOI to incorporate changes and add new features to the firewall protecting the Livescan system.

Further, DOI does not adequately monitor security violations as it has no procedure in place to ensure that violations are documented and reviewed. Such procedures would help DOI to identify patterns of security violations and to ensure that proper controls are instituted to prevent unauthorized access to Livescan. Directive 18, § 11.5, states that “a review of security violations will highlight unresolved problems or weaknesses in internal controls and may show patterns of failure and abuse requiring remedial action.”

Moreover, although DOI has undergone organizational changes, its security documentation has not been periodically updated. For example, the documentation refers to computer personnel who no longer work for DOI. Obviously, these individuals should have been removed from the documentation. As another example, the documentation refers to responsibilities of the Division of Information Systems and Computers. This unit, however, was split into two separate units— CISAFE and Information Technology. It is important for DOI to perform periodic updates to its security documentation to match the actual functions of its respective units.

DOI has an inadequate fire suppression system protecting Livescan at its Maiden Lane facility, and it could not provide documentation of its fire prevention efforts for its Chambers Street facility. Directive 18, § 7.0, states, “Protection from . . . damage by fire [and] water, . . . and loss of power are all elements of physical security.” During our walk-through, we noted that the Maiden Lane building’s sprinkler system uses water, not chemicals, to extinguish fires. Because water could damage the computer equipment, DOI should install a fire-suppression system that would protect the equipment.

Finally, DOI does not have access to the Livescan source code. Comnetix owns the code and maintains the system. According to DOI’s Chief Contracting Officer, in the event that Comnetix goes out of business or is otherwise unavailable, the agency could not support Livescan without having its source code, which would thereby necessitate the development of a replacement system.

Recommendations

DOI should:

1. Ensure that the Cardscan subsystem is operational and that appropriate personnel are trained in its operation.

DOI Response: “The Cardscan subsystem is fully operational and appropriate personnel are trained in its operation. In the event the Livescan scanner is not in service, the subsystem will be used to print out pedigree information and prints for the person to be fingerprinted.

“Operation of the Cardscan subsystem was demonstrated to the Comptroller’s auditors’ during the exit conference. A sample copy of the card produced by the subsystem is attached.”

Auditor Comment: At the exit conference, the Director of the Background, Vendex, Complaints, and Fingerprinting Unit demonstrated that Cardscan was operational. But at no time during the audit or at the exit conference did DOI demonstrate that appropriate personnel are trained in its operation or indeed that any users could operate Cardscan. Further, the Director agreed with the auditors that the users' ability to operate this module was never demonstrated and would be corrected.

2. Follow a formal systems-development methodology for all future systems-development projects and engage an independent quality assurance consultant or assign an employee to monitor and review development work, as well as any system enhancements to Livescan. In addition, DOI should develop formal acceptance-sign-off procedures to ensure that all system requirements are completed.

DOI Response: "Although no formal systems-development methodology was followed, the steps within the entire process could be mapped to a formal systems development methodology. For example, The US Department of Justice's System Development Life Cycle (SDLC), has 10 phases: (1) Initiation, (2) System Concept Development, (3) Planning, (4) Requirements Analysis, (5) Design, (6) Development, (7) Integration and Test, (8) Implementation, (9) Operations and Maintenance, and (10) Disposition. All of the documents provided to the Comptroller's Office by DOI beginning with the letter to the OMB Budget Director by the former DOI Deputy Commissioner for Administration defining the problem and the project scope, in our opinion, can be mapped perfectly to the first four phases of DOJ's SDLC. Phases 5 and 6 are a combination of DCJS's and the Vendor's responsibilities as found in the DCJS Civil Fingerprinting System (CFS)_Requirements Document and the Comnetix Certified Applicant Processing System (CAPS) Record Transfer Interface document, which contains the data definition specifications per NIST, the State and the FBI. Phases 7 and 8 can be found on Page 10 of the DCJS Civil Fingerprint System (CFS) Requirements Document. Phase 9 responsibilities are shared by the technical, operations and development staff of DCJS, the software vendor and DOI. Phase 10 can be mapped to the Livescan archival process explained in the DOI Disaster Recovery/Business Continuity Plan. DCJS specifies the changes and enhancements to the system, and the software vendor has to adhere to those specifications.

"Attached is a statement from DCJS dated 2/23/04, indicating that DOI successfully completed the 'Interagency Test Plan for Civil Store and Forward.'

"As a result, of the completion of the testing, DOI's plan for production implementation was approved.

"DOI is committed to adopting the U.S. Department of Justice's System Development Life Cycle guidelines for all future systems development projects. Furthermore, inasmuch as engaging the services of a Quality Assurance Consultant is not feasible at this time due to the current fiscal situation, DOI will assign an agency employee to monitor and review new development work, as well as, any system enhancements to

Livescan. Formal acceptance sign-off procedures will be developed and implemented to ensure that all system requirements are completed in accordance with specified SDLC guidelines.”

Auditor Comment: DOI agrees with the report’s finding that no formal methodology was followed and also agrees to implement the audit’s recommendation, but indicates that the entire process could be mapped to the U.S. Department of Justice’s System Development Life Cycle methodology. What DOI must understand is that following a specific methodology from the beginning is quite different from showing a process *after* the project is completed. A system-development methodology allows the project manager and the project team to manage the development on a systematic, day-to-day basis, thereby linking the project’s development to a given set of expectations (deliverables and due dates) and at the same time significantly alleviating the risks inherent in agency systems development projects. Such methodologies help to ensure that system development efforts are conducted in a structured, logical, organized, and efficient manner and that systems meet their objectives.

3. Develop procedures to determine whether an event is sufficiently serious to invoke its disaster recovery plan. In addition, DOI should formalize agreements with the vendors to provide software supplies and equipment and with DoITT regarding the alternate processing site. Finally, DOI should periodically test the disaster recovery plan.

DOI Response: “DOI’s Information Technology (IT) Unit has developed a Disaster Recovery/Business Continuity Plan, in accordance with the procedures set forth in Comptroller’s Directive 18, Section 10. DOI currently has formalized contract agreements (referred to as Requirements Contracts) with all Vendors it utilizes to provide software supplies and equipment. Appendix G of the Disaster Recovery Plan contains a list of approved vendors and their respective products (hardware and software) along with their telephone number, contract/service agreement numbers, and expiration date.

“DOI will seek to formalize an agreement with DoITT concerning an alternate processing site. Once established, the warm site will be equipped with all the hardware and software needed to recover business operations. IT unit staff will be responsible for installation and maintenance of all equipment.

“DOI will conduct periodic testing of its disaster recovery plan using mock scenarios to ensure that it works properly. Adjustments to the plan will be made as needed.”

Auditor Comment: DOI indicates that it has developed a Disaster Recovery/Business Continuity Plan, but later states in its response that it will seek to formalize an agreement with DoITT concerning an alternate processing site and will conduct periodic testing of its plan. For a plan to be complete, all facets of the plan must be in force and tested. That said, DOI must still complete the open items mentioned before its plan can be complete.

4. Address the user concerns revealed in our survey. In that regard, DOI should consider including help menus and screens and formats that are easier to use and providing additional training to those users who reported that they had limited knowledge of the system.

DOI Response: “DOI will address user concerns revealed in the Comptroller’s survey by asking all unit staff if they require additional training. The unit head will subsequently provide training in those areas where staff indicate they are deficient. Additionally, the Livescan system has a help menu which staff can access as needed. It is not feasible to change screen formats, as the Livescan system must be in compliance with DCJS specifications.”

5. Ensure that its employees periodically change their passwords for Livescan and Secure Services.

DOI Response: “DOI has implemented a password policy for the Livescan workstations forcing unique password changes every 90 days. DOI has no control over the password policy for Secure Services which belongs to DCJS. Attached is an e-mail from Connie Snyder, DCJS, dated 3/3/04, indicating that there is no automatic password aging in the e-justice system. However, DCJS has recently purchased a new security system that includes the feature to automatically expire passwords and notify users. Implementation of the security system is in the works, although no definite date has been set by DCJS.”

6. Upgrade its CISCO PIX firewall version to the standards set by its CISAFE unit.

DOI Response: “DOI will be upgrading the CISCO PIX firewall software versions during the routers and switches rollout in April, 2004, thereby bringing it into compliance with the standards set forth by the agency’s Citywide Information Security Architecture Formulation Enforcement (CISAFE) unit.”

7. Establish formal procedures to document and report system-access violations, and review and follow up on all reported violations. In addition, DOI should ensure that maintenance of security documentation is accurate and complete.

DOI Response: “All of these issues will be addressed with the Workstation Server rollout scheduled to be completed in March, 2004. There is firewall and intrusion detection software in the workstations that will maintain a log of such incidents on the workstation. Moreover, DOI will implement an intrusion detection system on the network for traffic analysis and on servers for host-based analysis. In addition, DOI will ensure that maintenance of security documentation is accurate and complete.”

8. Install a fire-suppression system that would protect the equipment. In addition, DOI should document the fire prevention procedures in effect at its Chambers Street facility.

DOI Response: “In response to this recommendation DOI contacted George Sultana, Executive Director, Facilities Operations, Department of Citywide Administrative Services (DCAS). According to Mr. Sultana, DCAS would need to perform a feasibility study through its engineering staff to evaluate whether it is possible to install a fire suppression system. Based upon his knowledge, Mr. Sultana indicated that such a system would be prohibitively expensive. However, DOI will continue to seek information as it relates to cost and feasibility prior to making a final determination. It should be noted that this is not considered a critical function of the Department, as fingerprinting could be performed at an alternate location if necessary.

“According to Mr. Sultana, the 49-51 Chambers Street Facility has a stand pipe and fire alarm in the lobby of the building which is in compliance with Fire Department code. There are fire extinguishers located within the confines of the Fingerprint Unit in close proximity to the Livescan system.”

9. Obtain the Livescan source code in case the vendor should become unavailable.

DOI Response: “DOI will explore the possibility of negotiating an amendment to the Lifescan contract with Comnetix, wherein the company would be asked to turn over the source code for the Lifescan project in the event it goes out of business. Alternatively, DOI would ask Comnetix to train IT staff using system documentation. Enforcement of the terms of the amendment will be explored with the agency’s General Counsel.”



The City of New York
Department of Investigation

ROSE GILL HEARN
COMMISSIONER

80 MAIDEN LANE
NEW YORK, NY 10038
212-825-5900

March 19, 2004

Greg Brooks
Deputy Comptroller
Policy, Audits, Accountancy & Contracts
Office of the Comptroller
Executive Offices
1 Centre Street
New York, NY 10007

Re: Audit Report on the Development and Implementation of the Department of Investigation ("DOI") Livescan Fingerprint System (7A04-067)

Dear Mr. Brooks:

This letter is in response to the draft audit report issued by the Comptroller's Office, dated March 5, 2004, pursuant to its audit on the Development and Implementation of the Department of Investigation's Livescan Fingerprint System (7A04-067). As requested, included below, are DOI's responses to the Comptroller's recommendations.

Recommendation:

1. Ensure that the Cardscan subsystem is operational and that appropriate personnel are trained in its operation.

DOI Response:

The Cardscan subsystem is fully operational and appropriate personnel are trained in its operation. In the event the Livescan scanner is not in service, the subsystem will be used to print out pedigree information and prints for the person to be fingerprinted.

Mr. Greg Brooks
Re: Audit Livescan Fingerprint System
March 19, 2004
Page 2

Operation of the Cardscan subsystem was demonstrated to the Comptroller's auditors' during the exit conference. A sample copy of the card produced by the subsystem is attached.

Recommendation:

2. Follow a formal systems-development methodology for all future systems-development projects and engage an independent quality assurance consultant or assign an employee to monitor and review development work, as well as any system enhancements to Livescan. In addition, DOI should develop formal acceptance-sign-off procedures to ensure that all system requirements are completed.

DOI Response:

Although no formal systems-development methodology was followed, the steps within the entire process could be mapped to a formal systems development methodology. For example, The US Department of Justice's System Development Life Cycle (SDLC), has 10 phases: (1) Initiation, (2) System Concept Development, (3) Planning, (4) Requirements Analysis, (5) Design, (6) Development, (7) Integration and Test, (8) Implementation, (9) Operations and Maintenance, and (10) Disposition. All of the documents provided to the Comptroller's Office by DOI beginning with the letter to the OMB Budget Director by the former DOI Deputy Commissioner for Administration defining the problem and the project scope, in our opinion, can be mapped perfectly to the first four phases of DOJ's SDLC. Phases 5 and 6 are a combination of DCJS's and the Vendor's responsibilities as found in the DCJS Civil Fingerprinting System (CFS)_Requirements Document and the Comnetix Certified Applicant Processing System (CAPS) Record Transfer Interface document, which contains the data definition specifications per NIST, the State and the FBI. Phases 7 and 8 can be found on Page 10 of the DCJS Civil Fingerprint System (CFS) Requirements Document. Phase 9 responsibilities are shared by the technical, operations and development staff of DCJS, the software vendor and DOI. Phase 10 can be mapped to the Livescan archival process explained in the DOI Disaster Recovery/Business Continuity Plan. DCJS specifies the changes and enhancements to the system, and the software vendor has to adhere to those specifications.

Attached is a statement from DCJS dated 2/23/04, indicating that DOI successfully completed the "Interagency Test Plan for Civil Store and Forward."

Mr. Greg Brooks
Re: Audit Livescan Fingerprint System
March 19, 2004
Page 3

As a result, of the completion of the testing, DOI's plan for production implementation was approved.

DOI is committed to adopting the U.S. Department of Justice's System Development Life Cycle guidelines for all future systems development projects. Furthermore, inasmuch as engaging the services of a Quality Assurance Consultant is not feasible at this time due to the current fiscal situation, DOI will assign an agency employee to monitor and review new development work, as well as, any system enhancements to Livescan. Formal acceptance sign-off procedures will be developed and implemented to ensure that all system requirements are completed in accordance with specified SDLC guidelines.

Recommendation:

3. Develop procedures to determine whether an event is sufficiently serious to invoke its disaster recovery plan. In addition, DOI should formalize agreements with the vendors to provide software supplies and equipment and with DoITT regarding the alternate processing site. Finally, DOI should periodically test the disaster recovery plan.

DOI Response:

DOI's Information Technology (IT) Unit has developed a Disaster Recovery/Business Continuity Plan, in accordance with the procedures set forth in Comptroller's Directive 18, Section 10. DOI currently has formalized contract agreements (referred to as Requirements Contracts) with all Vendors it utilizes to provide software supplies and equipment. Appendix G of the Disaster Recovery Plan contains a list of approved vendors and their respective products (hardware and software) along with their telephone number, contract/service agreement numbers, and expiration date.

DOI will seek to formalize an agreement with DoITT concerning an alternate processing site. Once established, the warm site will be equipped with all the hardware and software needed to recover business operations. IT unit staff will be responsible for installation and maintenance of all equipment.

DOI will conduct periodic testing of its disaster recovery plan using mock scenarios to ensure that it works properly. Adjustments to the plan will be made as needed.

Mr. Greg Brooks
Re: Audit Livescan Fingerprint System
March 19, 2004
Page 4

Recommendation:

4. Address the user concerns revealed in our survey. In that regard, DOI should consider including help menus and screens and formats that are easier to use and providing additional training to those users who reported that they had limited knowledge of the system.

DOI Response:

DOI will address user concerns revealed in the Comptroller's survey by asking all unit staff if they require additional training. The unit head will subsequently provide training in those areas where staff indicate they are deficient. Additionally, the Livescan system has a help menu which staff can access as needed. It is not feasible to change screen formats, as the Livescan system must be in compliance with DCJS specifications.

Recommendation:

5. Ensure that its employees periodically change their passwords for Livescan and Secure Services.

DOI Response:

DOI has implemented a password policy for the Livescan workstations forcing unique password changes every 90 days. DOI has no control over the password policy for Secure Services which belongs to DCJS. Attached is an e-mail from Connie Snyder, DCJS, dated 3/3/04, indicating that there is no automatic password aging in the e-justice system. However, DCJS has recently purchased a new security system that includes the feature to automatically expire passwords and notify users. Implementation of the security system is in the works, although no definite date has been set by DCJS.

Recommendation:

6. Upgrade its CISCO PIX firewall version to the standards set by its CISAFE unit.

DOI Response:

DOI will be upgrading the CISCO PIX firewall software versions during the routers and switches rollout in April, 2004, thereby bringing it into compliance with the standards set forth by the agency's Citywide Information Security Architecture Formulation Enforcement (CISAFE) unit.

Mr. Greg Brooks
Re: Audit Livescan Fingerprint System
March 19, 2004
Page 5

Recommendation:

7. Establish formal procedures to document and report system-access violations, and review and follow up on all reported violations. In addition, DOI should ensure that maintenance of security documentation is accurate and complete.

DOI Response:

All of these issues will be addressed with the Workstation Server rollout scheduled to be completed in March, 2004. There is firewall and intrusion detection software in the workstations that will maintain a log of such incidents on the workstation. Moreover, DOI will implement an intrusion detection system on the network for traffic analysis and on servers for host-based analysis. In addition, DOI will ensure that maintenance of security documentation is accurate and complete.

Recommendation:

8. Install a fire-suppression system that would protect the equipment. In addition, DOI should document the fire prevention procedures in effect at its Chambers Street facility.

DOI Response:

In response to this recommendation DOI contacted George Sultana, Executive Director, Facilities Operations, Department of Citywide Administrative Services (DCAS). According to Mr. Sultana, DCAS would need to perform a feasibility study through its engineering staff to evaluate whether it is possible to install a fire suppression system. Based upon his knowledge, Mr. Sultana indicated that such a system would be prohibitively expensive. However, DOI will continue to seek information as it relates to cost and feasibility prior to making a final determination. It should be noted that this is not considered a critical function of the Department, as fingerprinting could be performed at an alternate location if necessary.

According to Mr. Sultana, the 49-51 Chambers Street facility has a stand pipe and fire alarm in the lobby of the building which is in compliance with Fire Department code. There are fire extinguishers located within the confines of the Fingerprint Unit in close proximity to the Livescan system.

Mr. Greg Brooks
Re: Audit Livescan Fingerprint System
March 19, 2004
Page 6

Recommendation:

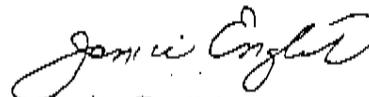
9. Obtain the Livescan source code in case the vendor should become unavailable.

DOI Response:

DOI will explore the possibility of negotiating an amendment to the Lifescan contract with Comnetix, wherein the company would be asked to turn over the source code for the Lifescan project in the event it goes out of business. Alternatively, DOI would ask Comnetix to train IT staff using system documentation. Enforcement of the terms of the amendment will be explored with the agency's General Counsel.

I would like to take this opportunity to thank your staff for their graciousness during the entire audit process. Should you have any questions with respect to DOI's response to the findings and recommendations, please contact Ana E. Albino, Audit Coordinator, at (212) 825-2400.

Very truly yours,



Janice English
Deputy Commissioner

Attachments

cc: Rose Gill Hearn, Commissioner

Attachment 1 - Recommendation # 1

APPLICANT

SIGNATURE OF PERSON FINGERPRINTED

RESIDENCE OF PERSON FINGERPRINTED

5 - 29 56TH AVENUE, LONG ISLAND CITY, NY, US

DATE 02.19.2004

STRUCTURE OF OFFICIAL, FAMILY FINGERPRINTS

EMPLOYER AND ADDRESS

NYC DOJ ITT

REASON FINGERPRINTED
EDIT THIS DEFAULT IN CONFIRMLIST

ALIAS AKA

NY030011Y

DEPT OF INVESTIGATION

DATE OF BIRTH 01-12-1957

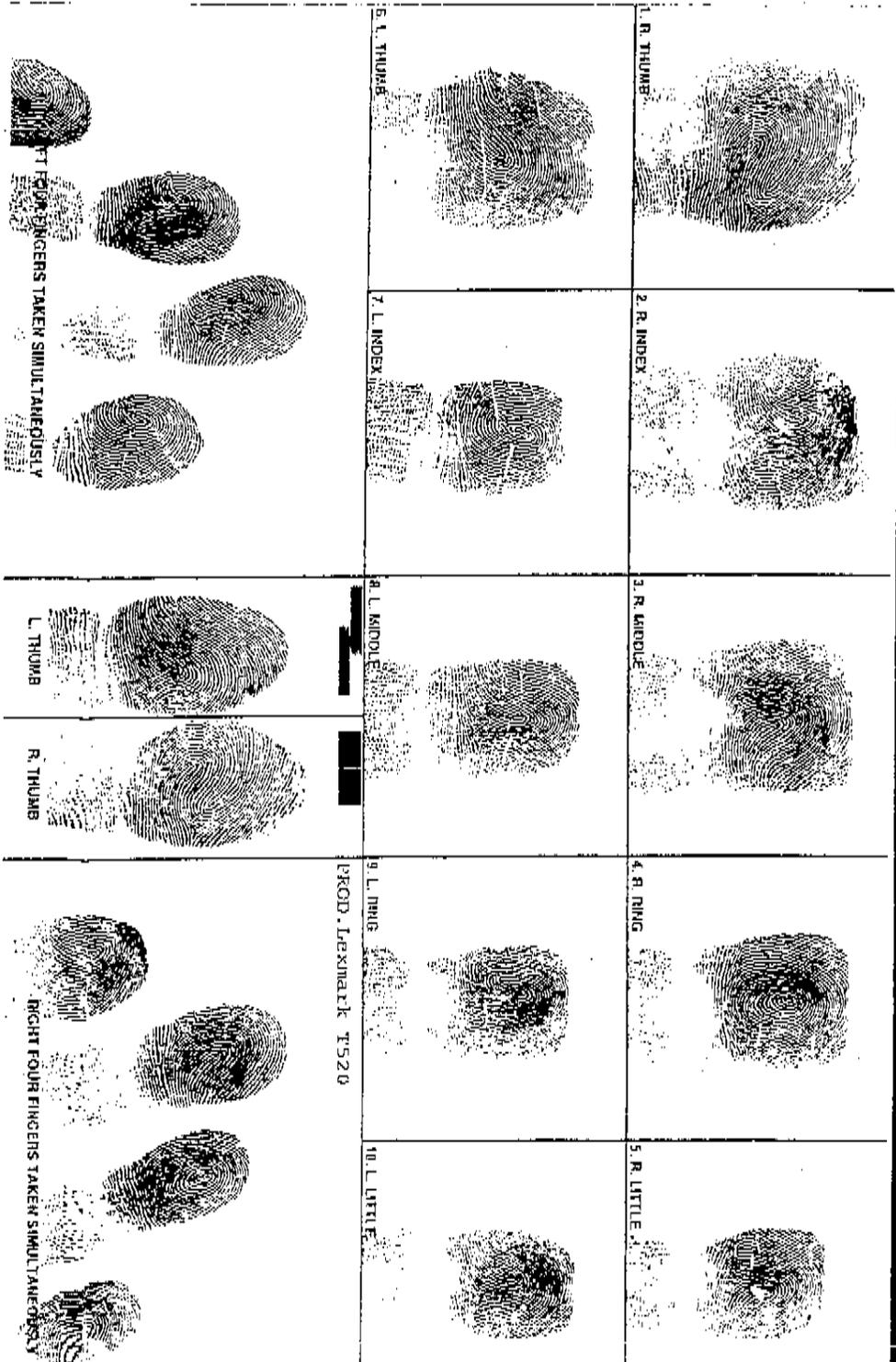
SEX F RACE W HGT 508 WGT 170 EYES GRN HAIR BRO

CLASS

LEAVE BLANK

POB NY

52 THE 45th STREET, NYC
MISCellaneous NO. MANU



LEFT FOUR FINGERS TAKEN SIMULTANEOUSLY

RIGHT FOUR FINGERS TAKEN SIMULTANEOUSLY

PCRD - Lexmark T520

3. Sheet No. [REDACTED] 3A. Street Address 5-29 5-01 E AVENUE

4. City/State Address LONG ISLAND NY

7. Alias or Maiden Name

8. Sex F 9. Race W 10. Hair BRO 11. Eyes GRN 12. Weight 170

11. Height In 51 12. Date of Birth Mo 01 Day 12 Yr. 37 13A. Age 37 13. Place of Birth (State or Country) NY

16. Agency I.D. # 2004000141 17. Social Security No. [REDACTED]

15. Date of Death Mo. Day Yr. 18. Date of Fingerprinted Mo. Day Yr. 0 2 1 8 0 4

21. REASON FOR FINGERPRINTED (Check One)
 Job Application
 License Application
 Police Off. Application
 Pistol License (63)
 Peace Off. Application
 Dead (62)
 Other _____

22. Type of Pistol License
 Dealer/Commission
 Possess
 Carry

24. Company, Agency, Department or Institution - name and address

25. _____

26. Signature of Person Fingerprinted

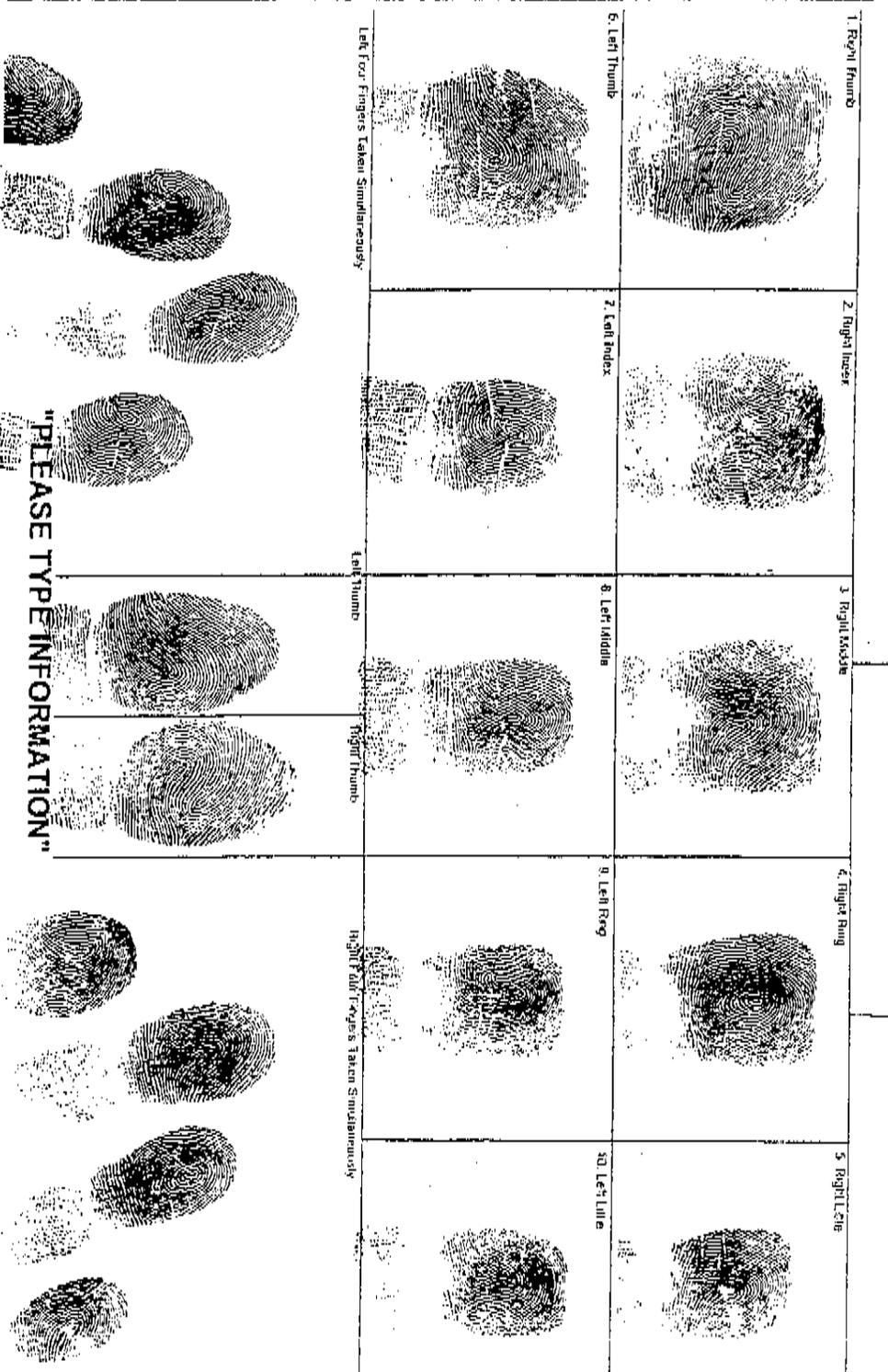
27. Immediate name and NYSID No.

28. Violent Felony/Offense to Inmate

29. Signature of Person Taking Prints

23. License Type/Job Title

23A. _____



From: "Giammattei, Cindy (DCJS)" <Cindy.Giammattei@dcjs.state.ny.us>
To: <ptierney@doi.nyc.gov>
Date: 2/23/04 11:03AM
Subject: Store and Forward Testing

According to documentation maintained in our files, NYC Dept of Investigation Management Background Unit participated in Store and Forward interagency testing with DCJS during the period 5/20/2002 through 5/22/2002. The NYC Dept of Investigation Child Care Unit participated in Store and Forward interagency testing with DCJS during the period 5/24/2002 through 5/28/2002.

As a result of successful completion of that testing as well as the successful quality review of the fingerprint images submitted during that test, DOI's plan for production implementation was approved.

Cindy Giammattei
NYS DCJS- QA Group
Ph: 518.485.0083
cindy.giammattei@dcjs.state.ny.us

Attachment 2 - Recommendation #2

NYS Division of Criminal Justice Services (DCJS) Interagency Test Plan for Civil Store and Forward (S&F)

Before Testing Can Begin:

DCJS staff will assign a test time frame, or window, for your agency to test with us prior to implementing Store & Forward processing in production. Your agency must complete all steps on the document titled "Checklist for Store and Forward Livescan/Cardscan Interagency Test Readiness" prior to getting approval to begin testing.

On the day that testing is scheduled to start, please contact the DCJS QA Unit at (518) 485-0083 or 0082 to make sure that the system is up and ready before you send the first transaction. You will generate transactions based on criteria in the test scripts, below. To the extent that it's practicable, please send test transactions in the exact manner that you will be using when you go to production and utilize personnel who will be involved in the production environment (not vendor or supervisory staff).

General Information (Refer to the EFTS for detailed information):

Upon receipt of a S&F transaction, DCJS will respond with either an acknowledgment that the transaction was received (SREACK) or an error response (ERRREJ) if the transaction contained an error. *Note:* All mandatory fields, per the EFTS document, must be completed with valid data for a transaction to be accepted.

If the transaction was initially accepted, the fingerprint card(s) will print at DCJS and the required fee will be assessed. Each civil type that is permitted, but not required, by law to include an FBI card submission must indicate whether an FBI submission should be processed by use of the appropriate EFTS tag. Each fingerprint card transaction printed will be reviewed for image quality by DCJS staff who will process the transaction if the print quality is acceptable. If the fingerprint quality review determines that the fingerprint images are deficient, DCJS staff will reject the transaction and you must send a resubmission with good prints.

If the transaction was initially rejected, there are data errors which you must correct before resubmission. (The one exception is a transaction that is rejected because it's a duplicate. Obviously, there should be no resend for that). When a transaction is initially rejected, the fee may be assessed at that point; if not, it will be assessed when the resubmission is processed, depending upon the particular error.

Once a print is accepted and processed, a processing results message will be returned (SRENY); a NYSID number will be included *except* when the input transaction was a search and return submission that did not result in an identification.

Note: Some tests, flagged with an asterisk, are designed to include data errors. If you have trouble entering these due to your system's edits, please discuss with DCJS test staff.

We suggest, but certainly don't require, using subject names which indicate the test being sent, as we've found that it helps in keeping organized. For test #1, send last name ONE and first name TEST, for test #2 send last name TWO and first name TEST, etc. For test 13 (which includes multiple cards), send the first record as last name THIRTEEN, first name ONE, the second record as last name THIRTEEN, first name TWO, etc.

Test Scripts

1. Type: Civil Job License Applicant
Purpose: Ensure all system components/applications are operational, the transaction can be processed, all messages are received.
Contributor: Transmit a civil transaction with no errors, the appropriate civil type, and good fingerprint images. Ensure that all data fields are completed, including Alias and Contributor Comments.
DCJS: Return SREACK, print fingerprint card. Determine that images are acceptable. Fully process the transaction and send a processing result (non-ident).
Contributor: Confirm the NYSID in the DCJS processing result.

TCN: _____

NYSID # from DCJS Processing Result: _____

2. Type: Civil Job/License Applicant
Purpose: Ensure that each of your agency's approved civil types can be sent and processed.
Contributor: Transmit a separate Civil Job/License Applicant transaction with each permitted civil type, and good fingerprint images. (See Appendix A.) For any civil types where submission of the FBI card is discretionary, submit one transaction with the FBI card and one without.
DCJS: Return SREACK, print fingerprint card. Determine that images are acceptable. Fully process the transaction and send a processing result (ident).
Contributor: Confirm the NYSID in the DCJS processing result, and FBI number if applicable.

TCN: _____

NYSID # from DCJS Processing Result: _____

3. Type: Civil Job/License Applicant
Purpose: Ensure that the contributor can transmit an applicant's NYSID number to DCJS and can store the NYSID received in the processing result, if different.
Contributor: Transmit a Civil Job/License Applicant transaction, including a NYSID number, with no errors and good fingerprint images.
DCJS: Return SREACK, print fingerprint card. Determine that images are acceptable and fully process the transaction. The input NYSID is not hit. Send a processing result with a different NYSID.
Contributor: Confirm that the NYSID in the DCJS processing result message is stored.

TCN: _____

NYSID # from DCJS Processing Result: _____

4. Type: Civil Job License Applicant
Purpose: Ensure that multiple rejections and resubmissions of a transaction can be handled.
Contributor: Transmit a Civil Job License Applicant transaction with a data error (e.g., a required field, such as Sex or Race, is missing or the first name is invalid) and fingerprint images with quality deficiencies. You will receive an ERRREJ message from DCJS. Correct the data error and resend the transaction with the poor quality images.
DCJS: Return SREACK, print fingerprint card. Images are reviewed by DCJS staff and found to be deficient. Transaction is rejected; ERRREJ is returned to contributor.
Contributor: Receive ERRREJ message. Resubmit the transaction with good quality fingerprint images.
DCJS: Return SREACK, print fingerprint card. Determine that images are acceptable. Fully process the transaction and send a processing result (ident).
Contributor: Confirm the NYSID in the DCJS processing result.
- 1st TCN: _____
2nd TCN: _____
3rd TCN: _____
- NYSID # from DCJS Processing Result: _____

5. Type: Civil Job/License Applicant
Purpose: For users of livescan systems, ensure that contributor can flag amped/bandaged fingers.
Contributor: Transmit an Civil Job/License Applicant transaction with no data errors. Send only 12 fingerprint images: mark the left ring finger (finger 9) as "amped" and the left little finger (finger 10) as "bandaged".
DCJS: Return SREACK, print fingerprint card. Determine that images are acceptable, and boxes with missing images are flagged. Fully process the transaction and send a processing result (ident).
Contributor: Confirm the NYSID in the DCJS processing result, and FBI number if applicable.
- TCN: _____
- NYSID # from DCJS Processing Result: _____

6. Type: Civil Job License Applicant
Purpose: Ensure that your system can handle receipt of a second processing result (SRENYS) with a different NYSID than was originally returned to you.
DCJS: Reject one of the previously completed civil transactions above that resulted in a non-ident. Use reject reason "SAFIS Restart" which will *not* initiate a ERRREJ message to the contributor. Reprocess the print and ident it to a NYSID number different from the one sent in the original process result response.
Contributor: Confirm that no ERRREJ message was received, that the new processing result message (SRENYS) was received and handled by your system, and that the new NYSID number was stored appropriately.

TCN: _____ Original NYSID#: _____

New NYSID # from DCJS Processing Result: _____

Electronic FBI Processing:

Perform this test only if your site will submit civil FBI transactions and any resubmissions of rejected FBI submissions to the FBI electronically, via Store and Forward.

NOTE: This functionality requires that your site use Secure Services for DCJS fingerprint response raps, notifications and electronic responses from the FBI.

- 7.* Type: Civil Job/License Applicant
Purpose: Ensure that multiple resubmissions of transactions rejected by the FBI can be processed.
Contributor: Submit a civil transaction with poor quality images.
DCJS: Return SREACK, print fingerprint card. Determine that images are acceptable. Fully process the transaction, store the multiple incident data, and send a processing result (non-ident). Return SRENYS. Modify the database to indicate that the FBI has rejected the transaction. Return ERRFBI.
Contributor: Resubmit the FBI transaction with new fingerprint images.
DCJS: Modify the database to indicate that the FBI has rejected the transaction. Return ERRFBI.
Contributor: Resubmit the FBI transaction with new fingerprint images.
DCJS: Return SREFBI.

Fingerprint Quality and Accuracy tests:

8. Type: Civil Job/License Applicant
Purpose: For users of livescan systems, ensure that your system will alert the person taking fingerprints if fingers are rolled out of order. (Note: DCJS will reject transactions with fingers rolled out of order.)
Contributor: Roll fingers out of sequence and ensure that your software catches the error. Reroll the images and transmit the "corrected" card.
DCJS: Return SREACK, print fingerprint card. Ensure that the images are in the proper order.

TCN: _____

9. Type: Civil Job License Applicant
Purpose: Ensure that your system will generate fingerprints of acceptable quality.
Contributor: Transmit 10 transactions using images from individuals known to be on the SAFIS system at DCJS.
DCJS: Return SREACK and print fingerprint card for each of the 10 transactions. Search the images against the database and obtain NYSID numbers.
Contributor: Confirm each of the 10 NYSID numbers to test image accuracy.

TCN#1:	_____	NYSID#	_____
TCN#2:	_____	NYSID#	_____
TCN#3:	_____	NYSID#	_____
TCN#4:	_____	NYSID#	_____
TCN#5:	_____	NYSID#	_____
TCN#6:	_____	NYSID#	_____
TCN#7:	_____	NYSID#	_____
TCN#8:	_____	NYSID#	_____
TCN#9:	_____	NYSID#	_____
TCN#10:	_____	NYSID#	_____

From: "Snyder, Connie (DCJS)" <Connie.Snyder@dcjs.state.ny.us>
To: <ptierney@doi.nyc.gov>
Date: 3/3/04 2:41PM
Subject: Password Aging

Peg, to followup on our phone conversation, currently there is no automatic password aging in the ejustice system. We have, however, just recently purchased a new security system that does include the feature to automatically expire passwords and notify our users of this. There is no definite timeframe for the implementation of this system but it is in the 'works'.

Connie Snyder
Chief, Enterprise Development
NYS Division Of Criminal Justice Services
connie.snyder@dcjs.state.ny.us
(518)485-7928
(518)457-1237(fax)

Attachment 3 - Recommendation #5