SAFIS Training Guide

SAFIS Program Team

- Executive Office of Public Safety and Security
  Boston, MA.

- Massachusetts State Police (MSP) State Identification Section (SIS)
  Sudbury, MA.

- Massachusetts Department of Criminal Justice Information Services (DCJIS) Chelsea, MA.

What is the Executive Office of Public Safety and Security (EOPSS)?

- EOPSS is one of 7 Executive Branch Secretariats.
- The Secretary of Public Safety and Security is a member of the Governor's cabinet.
- EOPSS oversees the 13 state public safety agencies within the Executive Branch.
- EOPSS is the manager of the contract with IdentoGO® by IDEMIA to provide fingerprint enrollment services across the state.

What is the Massachusetts State Police State Identification Section (SIS)?

- The SIS is a bureau within the Massachusetts State Police's Administrative Services Division.
- The SIS manages and operates the state's Automated Fingerprint Identification System (AFIS).
- Applicant fingerprints taken at IdentoGO® by IDEMIA centers are electronically forwarded to the SIS AFIS for processing; fingerprint submissions are compared to the existing fingerprint records within the AFIS database.

What is the Department of Criminal Justice Information Services (DCJIS)?

- The DCJIS is an agency within the Public Safety Secretariat.
- The DCJIS manages the state's Criminal Justice Information System (CJIS) and is also the designated FBI CJIS Systems Agency (CSA) for the Commonwealth.
- The DCJIS operates the SAFIS Unit, which is responsible for processing the results of state and national fingerprint-based background checks as well as for providing phone support for users of SAFIS-R.
- The DCJIS is responsible for conducting audits of non-criminal justice agencies which have access to criminal history record information (CHRI).
- DCJIS also provides CORI results in accordance with the CORI law to non-criminal justice agencies through the DCJIS iCORI system.

Definitions

- CHRI – Criminal History Record Information; generally, this term is used to describe fingerprint-supported criminal record information.
- CORI – Criminal Offender Record Information; the term used to describe criminal arraignment data compiled by the Massachusetts Trial Court; most of this data is not fingerprint supported.
- SAFIS – Statewide Applicant Fingerprint Identification Services; the program created by Massachusetts to process fingerprint-based criminal record checks for authorized Massachusetts non-criminal justice organizations.

Definitions (cont'd)

- SAFIS-R - Statewide Applicant Fingerprint Identification Services-Results; the internet-based application through which users access the results of fingerprint-based criminal record checks.

- SAFIS-R User – every organization must designate at least one, but no more than two, SAFIS-R Users who will be the recipient(s) of criminal record check results.

Federal Fingerprinting Authorization

- The following are federal laws authorizing fingerprint-based CHRI background checks for licensing or employment determinations:
  - Adam Walsh Act 42 U.S.C. 16962
  - Public Law 92-544

National Fingerprint Based Checks for Pre-K-12 Schools and Authorized Massachusetts State agencies

- Schools and school districts with legislation, regulations, and policy procedural questions about the state's fingerprinting law must contact the Department of Elementary and Secondary Education.
- Massachusetts State Agencies authorized to receive Fingerprint results with legislation, regulations, and policy procedural questions about the state's fingerprinting law must contact their specific agency.

Difference Between CHRI and CORI

CHRI	CORI
Fingerprint supported.	Not fingerprint supported.
Contains only offenses where an individual was fingerprinted.	Contains all offenses on which an individual was arraigned.
Contains information from all 50 states plus.	Contains only Massachusetts information.
Many records missing disposition data.	Contains complete disposition data.
May contain MA cases that have been sealed.	No sealed record data.

Criminal Justice Information Exchange

FBI Criminal Justice Information Services

Massachusetts Department of Criminal Justice Information Services (DCJIS)

Noncriminal Justice Agency

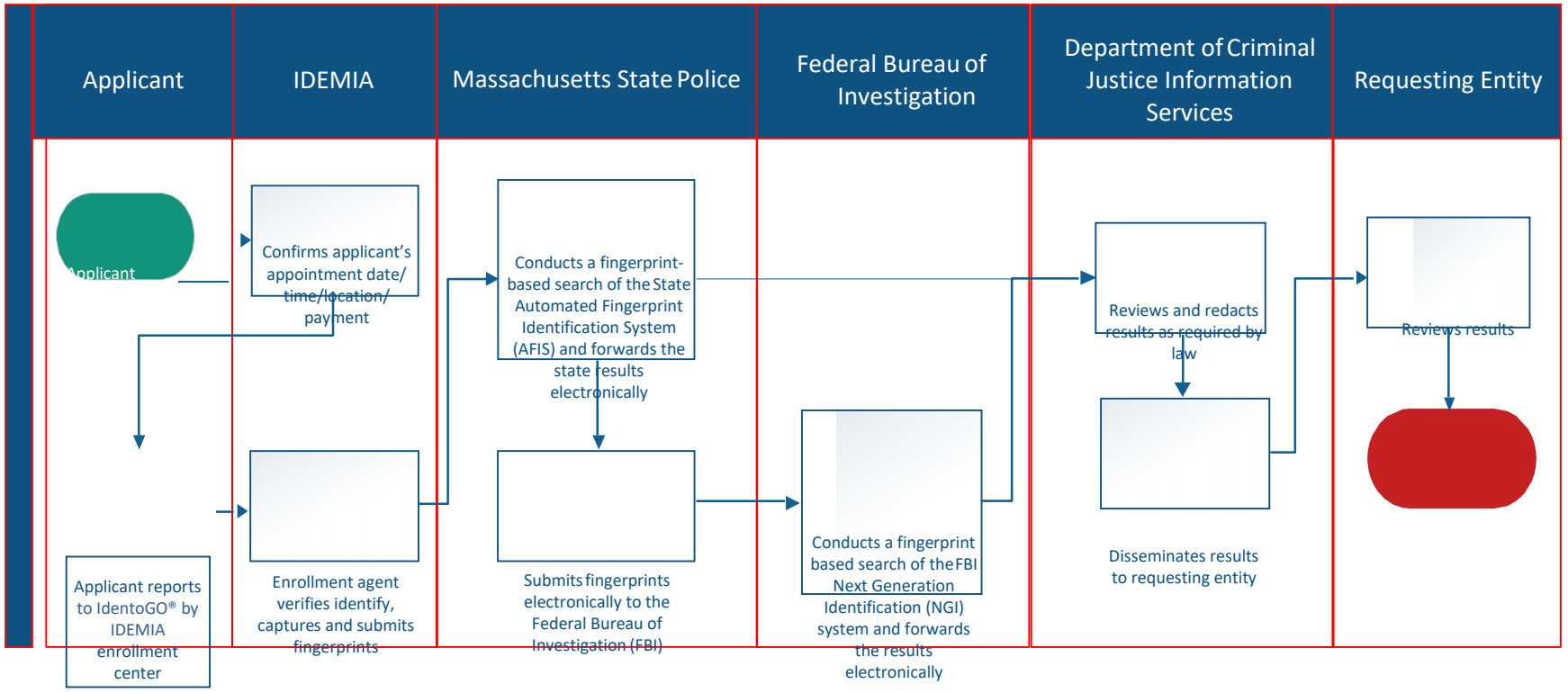
Serves as the nation's administrator for the appropriate security and management controls. As such, the FBI designates one criminal justice agency per state as the CJIS Systems Agency (CSA). The CSA is considered the point of contact in each state.

As the CSA for Massachusetts, the DCJIS is duly authorized to oversee the security and management of all Criminal Justice Information (CJI) exchanges within the state. The DCJIS is responsible for setting, maintaining, enforcing, and reporting compliance to the FBI CJIS Division for such exchanges.

For the purpose of licensing and employment, certain authorized agencies request and receive fingerprint based Criminal History Record Information (CHRI), making the Noncriminal Justice Agency (NCJA) the next responsible records management entity.

SAFIS Process Flow

Statewide Applicant Fingerprint Identification Services (SAFIS)



Applicants Have a Right to Due Process

- If an employer has obtained criminal history information about an applicant, regardless of the source, he or she must provide the criminal history to the applicant prior to asking him or her about it.

Restrictions on Dissemination of SAFIS Results

- Access to, and dissemination of, CHRI is regulated under 28 C.F.R. 20.33, the FBI CJIS Security Policy, and the laws applicable to the level of access afforded to the agency.
  - Organizations shall not disseminate CHRI outside of the requesting entity. The only current exception is that Department of Elementary and Secondary Education (DESE) entities can report CHRI data to DESE pursuant to its laws and regulations.
  - CHRI results may be shared with the subject of the CHRI.
  - CHRI may also be shared with individuals within the organization that have signed a non-disclosure agreement and completed the required training.
  - CHRI may not be repurposed. A new CHRI check must be requested when the purpose of the request has changed (i.e., promotion to a new position).

Sanctions and Penalties

- Improper access to, and/or dissemination of, CHRI may resultin any of the following:
  - loss of SAFIS-R access privileges.
  - civil fines and penalties issued by the DCJIS per M.G.L. c. 6, § 168 and 178, from $1,000 up to $5,000 per violation.
  - fines imposed by 28 C.F.R. 20.25, up to $11,000.
  - criminal prosecution per M.G.L. c. 6, §178 and M.G.L. c. 266, s. 120F.

Destruction of CHRI

- When any CHRI is no longer needed, it must be destroyed via shredding, burning, or some other means as to make the information completely unreadable.
- The agency shall sanitize, that is, overwrite at least three times or degauss, electronic media prior to disposal or release for reuse by unauthorized individuals. Inoperable electronic media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel.

Local Agency Security Officer- LASO

- Designated by the NCJA:
  - can be the HR Director or any other designee.
  - acts as a point of contact with the DCJIS for security-related matters.
  - informs the DCJIS Information Security Officer (ISO) of any security incidents.

Physical Security/Controlled Area

- NCJAs must ensure that CHRI is secure at all times.
- CHRI must only be processed in controlled areas with limited access.
- Computers which provide access to CHRI data must not be logged in when unattended.
- Authorized users must not share Usernames and Passwords.
- Documents must not be left out in the open as they could be viewed by unauthorized individuals.
- Computer screens and CHRI must not be viewable by unauthorized individuals.
- File cabinets and record rooms must be locked when unattended.

Personnel Security

- NCJA's must have a written process in place for the following:
  - any person with felony convictions shall be denied access to CHRI.
  - for a criminal record other than a felony, any person with an arrest without conviction or an individual believed to be a fugitive shall have their record reviewed to determine if access to CHRI is appropriate.
  - CHRI access will be discontinued for any person who is subsequently arrested or convicted of a crime and must be reported to the DCJIS before access may be reinstated.
  - support personnel, contractors, vendors, and custodial workers with access to areas during CHRI processing are subject to a fingerprint-based criminal background check unless escorted by authorized personnel at all times.

Personnel Security (cont'd)

- For authorized users with access to CHRI, the NCJA shall maintain written processes of the specific steps taken for the following:
  - the "immediate" termination of individual CHRI access upon termination of employment.
  - review of CHRI access authorizations upon individual reassignment or transfer.
  - a formal sanctions process for personnel with access to CHRI failing to comply with agency-established information security policies and procedures.
- An NCJA Policy template is available for an agency's use and can be found here here.

Media Protection

- NCJA's shall have an established policy and procedures for the appropriate security, handling, transporting, and storing of CHRI media. Each NCJA shall establish:
  - an overall electronic/physical media protection policy.
  - procedures restricting access to authorized personnel. Management controls are to exist for the processing and retention of CHRI media and for media to be secured in a controlled area.
  - procedures for transporting CHRI media from its original secured location to another. The policy must describe the steps taken to protect and prevent the compromise of the data in transit.
  - procedures for the appropriate disposal and sanitization of CHRI media when no longer needed, and the specific steps taken to protect and prevent CHRI media during the destruction process.

Incident Response

- Each NCJA shall establish an operational incident handling policy and procedures. Agencies are to ensure general incident response roles and responsibilities are included within the agency established and administered Security Awareness Training. Each NCJA shall establish:
  - information security reporting procedures outlining who to report to and how reporting happens through the agency chain of command upon discovery of any information security incident pertaining to CHRI.
  - incident handling capability procedures that include adequate preparation, detection, analysis, containment, eradication, recovery, and user response activities.

Incident Response (cont'd)

- Each NCJA shall establish:
  - procedures for the collection, retention, and presentation of evidence to the relevant law enforcement jurisdiction(s) for a CHRI security incident involving legal action (either civil or criminal) against a person or agency.
  - procedures to track, document, and report information security incidents. An "Information Security Officer (ISO) Computer Security Incident Response Capability Reporting," form (CJIS-016) has been established, and is the required method of reporting security incidents to the DCJIS.
- An NCJA Policy template is available for an agency's use and can be found here here.

Security Awareness Training

- Each NCJA shall have an established Security Awareness Training (SAT) program, approved by the CJIS Systems Officer (CSO) at the DCJIS.

NCJA Audits

- The FBI's CJIS Division conducts a triennial audit of each state on the use of CJI, including criminal history record information.
  - these audits will include randomly selected NCJAs

- The FBI and Massachusetts law also require the DCJIS to audit NCJAs. The DCJIS-conducted audits may occur in close proximity to any audits conducted by the FBI.

NCJA Audits (cont'd)

- DCJIS auditors will check for documentation to support the fingerprint background check:
  - evidence which indicates the fingerprint-based CHRI background checks obtained are for a specific purpose authorized by state or federal law.
  - position descriptions are formal agency documentation providing the individual's name and position offered by the agency (i.e. employment contracts, new hire checklist, letter of hire, determination for assignment etc.).

NCJA Audits (cont'd)

- Applicant appeal process
  - a formal appeal process for applicants wishing to challenge, correct, or update their criminal history record must be in place:
    - Organizations authorized to submit CHRI checks pursuant to state and federal laws are required to provide individuals with information on how to change, correct, or update their criminal records in accordance with 28 CFR 16.34.
    - Audits will review your appeals process to ensure individuals are being afforded the opportunity to change, correct, or update their criminal history.
    - Please see the DCJIS website for the form published by the Commonwealth that outlines how an individual can request to have his/her CHRI record updated, changed, or corrected.

Auditable Areas

- The following areas will be reviewed by the DCJIS auditors:
  - supporting documentation
  - Local Agency Security Officer (LASO) appointment
  - personnel security
  - media protection
  - physical security
  - incident response
  - secondary dissemination
  - Security Awareness training

NCJA User Agreement

- NCJA's receiving CHRI from the DCJIS *shall* complete a Noncriminal Justice Agency User Agreement for the Use of Criminal History Record Information.
- This formal agreement specifies how the exchange of CHRI is to be conducted between the DCJIS and the NCJA through applicable security and management controls:
  - outlines each party's individual roles and responsibilities as they pertain to the day to day receipt and processing of CHRI and all that it entails, including data ownership.
  - requires the authorized signature of the agency representative (an employee of the agency with explicit authority to commit the agency to the agreement).

Freedom of Information Act (FOIA)/Public Records Requests

- State and national CHRI is NOT considered public information and cannot be released:
  - CHRI is specifically exempt from disclosure under the Massachusetts Public Records law, M.G.L. c. 66, s. 10, under exemption M.G.L. c. 4, s.7 clause (26)(a) as "specifically or by necessary implication exempted from disclosure by statute". The specific statutes that exempt the public dissemination of this information include: M.G.L. c. 6, s. 172 and 28 C.F.R. 20.33.

Request Copy of a Background Check Response

- Background check responses are sent *only* to an organization's authorized SAFIS-R users. If a response is not received, an authorized user should contact the DCJIS SAFIS Unit:
  - Telephone: (617) 660-4790
  - Email: safis@mass.gov
- After six months from the time an applicant is fingerprinted, access to the results in the SAFIS-R system expires for registered SAFIS-R user retrieval.

SAFIS Contact Information

- SAFIS Website:

  http://www.mass.gov/eopss/agencies/safis/statewide-applicant-fingerprint-identification-services.html

- SAFIS Response Unit Contact Information:
  - Telephone: (617) 660-4790
  - Email: safis@mass.gov