Guide for Noncriminal Justice Agencies

Contents

Acronym Glossary

Acronym	Term
CHRI	Criminal History Record Information
CJI	Criminal Justice Information
CJIS	Criminal Justice Information Services
CSP	CJIS Security Policy
CSA	CJIS System Agency
FBI	Federal Bureau of Investigation
III	Interstate Identification Index
ISO	Information Security Officer
LASO	Local Agency Security Officer
LSP	Louisiana State Police
LSP Bureau	Louisiana State Police Bureau of Criminal Identification & Information
NAC	Noncriminal Agency Coordinator
NCJA	Noncriminal Justice Agency
NGI	Next Generation Identification
ORI	Originating Agency Identifier
OTS	Louisiana Division of Administration's Office of Technology Services
OTS ISP	Office of Technology Services Information Security Policy
SID	State Identification Number

Introduction

This guide was created to assist noncriminal justice agencies that submit fingerprints and receive criminal history record information for noncriminal justice purposes pursuant to authorizations allowed by state and federal law.

Overview & History

Federal Public Law 92-544, passed by Congress in October 1972, provided for funds to be allocated for the exchange of criminal history identification records for noncriminal justice purposes, pursuant to approved statutes. In 1998, the National Crime Prevention and Privacy Compact Act was passed allowing signatory states to exchange criminal history records for noncriminal justice purposes according to a uniform standard. The 1998 act also established the National Crime Prevention and Privacy Compact Council to regulate and assist in maintaining a method of exchange of criminal history record information which protects both public safety and individual privacy rights. The FBI Criminal Justice Information Services (CJIS) Division houses the largest repository of fingerprint-based criminal history records and is charged with the responsibility and authority to oversee the exchange of such records. Federal laws, regulations, and policies have been formed both to govern the release of information exchanges through the FBI and to require states to regulate access, use, quality, and dissemination of state-held records.

What is Criminal History Record Information (CHRI)?

The FBI maintains an automated database (Next Generation Identification or NGI) that integrates criminal history records submitted by federal, state, local, and tribal agencies. Each state has a criminal records repository responsible for the collection and maintenance of criminal history records submitted by law enforcement agencies in its state. The Louisiana State Police Bureau of Criminal Identification and Information (LSP Bureau) is the state's designated repository that stores criminal history record information (CHRI) in the Louisiana Computerized Criminal History (LACCH) database. The state record repositories are the primary source of CHRI maintained at the FBI.

CHRI is defined by Title 28 Code of Federal Regulations (CFR) §20.3 as information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, information, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, and release. 28 CFR §20.21 further states information is considered CHRI if it confirms the existence or nonexistence of CHRI. CHRI is also described by the FBI CJIS Security Policy 4.1.1 as a subset of Criminal Justice Information (CJI) and is sometimes referred to as "restricted data." Information is considered CHRI if it is transferred or reproduced directly from CHRI received as a result of a national FBI check and associated with the subject of the record. This includes information such as conviction/disposition data as well as identifiers used to index records regardless of format.

The FBI's NGI stores the world's largest and most efficient electronic repository of biometric and criminal history information. However, the FBI's NGI database may not contain some records stored in the LSP Bureau's repository. For example, a civil agency authorized by state law to receive records expunged in Louisiana's criminal history database will not receive the expunged record if only a federal background check is conducted in a manner that bypasses the LSP Bureau. Civil agencies must submit

fingerprints to the FBI via the LSP Bureau as required by Public Law 92-544 in order to receive the most complete and comprehensive response.

Criminal history information does not include driver history records or arrests in which the offender was issued a summons. All CHRI must be supported by a fingerprint submission taken at the time of arrest.

Access to Criminal History Record Information (CHRI)

Federal Criminal History Record Information (CHRI)

The authority for the FBI to conduct a criminal record check for a noncriminal justice licensing or employment purpose is based upon Public Law 92-544. Pursuant to this law, the FBI is empowered to exchange identification records with officials of state and local governments for purposes of licensing and employment if authorized by a state statute which has been approved by the Attorney General of the United States.

Public Law 92-544 Requirements:

The Attorney General's authority to approve the statute is delegated to the FBI by 28 C.F.R. § 0.85(j). The standards employed by the FBI in approving Pub. L. 92-544 authorizations have been established by a series of memoranda issued by the Office of Legal Counsel, Department of Justice. The standards are:

1. The authorization must exist as the result of legislative enactment (or its functional equivalent);
2. The authorization must require fingerprinting of the applicant;
3. The authorization must, expressly or by implication, authorize use of FBI records for screening of the applicant;
4. The authorization must not be against public policy;
5. The authorization must not be overly broad in its scope; it must identify the specific category of applicants/licensees.

Fingerprint submissions to the FBI under Pub. L. 92-544 must be forwarded through a state's identification bureau. La. Revised Statute (L.R.S.) 15:575 et seq. establishes the LSP Bureau as the designated identification bureau and criminal history record repository. The state must also designate an authorized governmental agency to be responsible for receiving and screening the results of the record check to determine an applicant's suitability for employment or licensing.

CHRI obtained under this authority may be used solely for the purpose for which the record was requested and shall not be shared with any other agency or entity, even if the agency or entity is authorized to receive CHRI pursuant to its own statutes. When CHRI is needed for a subsequent authorized use, a new record request including fingerprints must be submitted to obtain the most possible current and accurate information.

Once a state law is approved, the FBI issues an Originating Agency Identifier (ORI) number to the agency that must be associated with a fingerprint submission before federal CHRI is released.

Louisiana Criminal History Record Information (CHRI)

Louisiana Revised Statute 15:578 establishes the Louisiana Bureau of Criminal Identification and Information (LSP Bureau) as the central repository of CHRI in Louisiana. Duties of the LSP Bureau include but are not limited to:

1. Establish and implement a uniform system for reporting criminal history record information from any state or local criminal justice agency.
2. Adopt and promulgate regulations to protect the privacy and security of criminal history record information exchanged with the bureau by any state or local criminal justice agency.
3. Establish, maintain, and regulate a modern system of telecommunication and data processing for the efficient collection, storage, and rapid transmission of criminal history record information and relevant statistics maintained by the bureau. Serve qualified agencies concerned with the administration of criminal justice throughout the state.
4. Establish a system of fingerprint identification and analysis for use in the maintenance of criminal history record information; to aid in official investigations by eligible agencies; and to establish identification where authorized by law.

The LSP Bureau may only release CHRI stored in the Louisiana Computerized Criminal History (LACCH) database, the state's repository for CHRI, as authorized by a specific state law. Agencies authorized to receive CHRI from only the LACCH database but not the FBI's NGI must be issued a Criminal Records Unit (CRU) number assigned by the LSP Bureau prior to receiving CHRI.

Federal Policy references:

- 28 U.S.C. § 534 (a)(4)
- 34 U.S.C. § 40316, Article IV (c) and Article V (a) and (c)
- 28 C.F.R. § 20.33
- 28 C.F.R. § 50.12 (b)
- 28 C.F.R. § Part 901
- Public Law 92-544

Louisiana Revised Statute references:

- L.R.S. 15:577 Creation of the Bureau of Criminal Identification and Information
- L.R.S. 15:579 Rules and Regulations
- L.R.S. 15:595 Duty to Abide by Regulations
- L.R.S. 15:596 Penalties

Reason Fingerprinted Field and Purpose Code Usage

The privacy Act of 1974 requires that the FBI's CJIS Division keep an accurate accounting of the purpose of each disclosure of a criminal history record and the recipient of that record. As such, all requests for civil background checks shall include the state's statutory authority by which the agency is authorized to receive CHRI. Additionally, each agency is required to record the appropriate Applicant Type Code assigned by the LSP Bureau as well as the specific job title that qualifies the authorized recipient of criminal history record information to request a state and federal fingerprint-based background check.

Policy reference:

- 5 U.S.C. § 522a, (c)(1)(A)

User Fees

Louisiana Revised Statute 15:587 B(1) enables the Bureau to charge a processing fee of $26.00 for access to criminal history record information for noncriminal justice purposes.

28 C.F.R. § 20.31 allows the FBI to collect fees for noncriminal justice fingerprint-based background checks. The Director of the FBI shall review the amount of the fee periodically, but not less than every four years, to determine the current cost of processing fingerprint identification records for noncriminal justice purposes. The current fee for a federal background check is $13.25. The Bureau collects this fee on behalf of the FBI and forwards the monies to them monthly.

FBI Criminal Justice Information Services (CJIS) Security Policy

The FBI's Criminal Justice Information Services (CJIS) Security Policy provides (CSP) guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of Criminal Justice Information (CJI). This policy applies to every individual-contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity-with access to, or who operate in support of, criminal justice services and information.

The CJIS Security Policy integrates presidential directives, federal laws, FBI directives and the criminal justice community's Advisory Policy Board decisions along with nationally recognized guidance from the National Institute of Standards and Technology. As use of criminal history record information for noncriminal justice purposes continues to expand, the CJIS Security Policy becomes increasingly important in the secure exchange of criminal justice records. The CJIS Security Policy provides a secure framework of laws, standards, and elements of published and vetted policies for accomplishing the mission across the broad spectrum of the criminal justice and noncriminal justice communities (Appendix A).

Civil Agency User Agreement

Pursuant to the CJIS Security Policy (CSP) 5.1.1.6 "Agency User Agreements", each agency authorized to receive criminal history record information (CHRI) must sign a User Agreement. A User Agreement is a contractual agreement between the authorized receiving agency and the LSP Bureau (Appendix B). The User Agreement contains Terms and Conditions which include the following:

Authority and Purpose: The User Agreement identifies the requesting Agency, identifies the purpose for which criminal justice history information is requested, and identifies the specific statutory authorization granting access to the information. N**oncriminal justice agencies are prohibited from using criminal history record information for any purpose other than that for which it was requested.**

Sanctions/Penalties: The User Agreement is subject to cancellation by either party with 14 days written notice. The LSP Bureau reserves the right to immediately suspend service for violation or for investigation of apparent/alleged violations of the User Agreement or requirements for access. State and federal civil and/or criminal penalties may apply for misuse of CHRI. CHRI must be used solely for the purpose requested and cannot be disseminated outside the receiving Agency.

CSP 3.2.9 Local Agency Security Officer (LASO): Pursuant to CSP 3.2.9, the User Agreement requires the appointment of a LASO to act as liaison with the LSP Bureau and the Division of Administration's Office of Technology Services (OTS) to ensure the agency is in compliance with security procedures. This

individual must be knowledgeable in CHRI policies and mandated rules and regulations as well as knowledge of IT security procedures (Appendix C). LASOs are designated as the point of contact on security-related issues for their respective agencies and LASOs are responsible for instituting the CJIS System Agency (CSA) incident response reporting procedures at their agency as needed (Appendix D). See the section titled "Incident Response" for more information related to the duties of the LASO.

Noncriminal Agency Coordinator (NAC): The chief official of each noncriminal justice agency will designate a NAC to act as the primary contact person for that agency (Appendix E). The NAC should complete LSP Bureau training requirements and shall serve as liaison between the agency and the LSP Bureau. The NAC will ensure all employees with access or potential access to CHRI successfully complete the appropriate level of CJIS Security Awareness Training and will maintain that certification as long as the employee may have access to CHRI. This requirement includes janitorial staff and personnel that work for contractors and vendors. The NAC will also assist LSP Bureau personnel with scheduled audits or any other LSP Bureau requests for information or assistance.

Duties of the NAC also include but are not limited to:

1. Authorized Personnel List: The NAC is responsible for maintaining an updated Authorized Personnel List on file with the LSP Bureau. The Authorized Personnel List contains those individuals whom the agency has identified as authorized to access, handle, and/or destroy CHRI. The authorizations are based solely on the agency's determination, but should be limited to the minimum number of personnel necessary. All personnel who view, handle, use, disseminate, or dispose of CHRI must appear on the list. Anyone included on this list must undergo the appropriate level of CJIS Security Awareness Training.
2. Agency File Information: The NAC should inform the LSP Bureau of changes in the agency head or any relevant business information (agency name changes, mailing/physical address changes, etc.). Changes must be made as they occur.
3. Authorization and Purpose: A change in an agency's authorization may invalidate the entire User Agreement; if the NAC becomes aware of a change in the authorization for access (e.g., new state statute, etc.), he/she shall contact the LSP Bureau immediately to update the User Agreement and, if necessary, submit the new authorization to LSP Bureau.

Misuse of CHRI: The exchange of the CHRI is subject to immediate cancellation if dissemination is made outside the receiving departments or related agencies and if CHRI is used for any other reason that is not stated in Louisiana law. Furthermore, depending upon the nature of the offense and the identity of the offender, federal or state crimes may be charged for the willful, unauthorized disclosure of CHRI. Misuse of the CHRI can be a misdemeanor or felony depending on the circumstances.

Penalties for Misuse of CHRI:

- 28 U.S.C. § 534 (b)
- Public Law 92-544
- 28 C.F.R. § 20.33(b) and (d)
- L.R.S. 15:596

Applicant Notification and Record Challenge

The National Crime Prevention and Privacy Compact Council (Compact Council) outlines rights provided to applicants who are the subject of a national fingerprint-based criminal history record check for a

noncriminal justice purpose. These rights are detailed in the Agency Privacy Requirements for Noncriminal Justice Applicants document (Appendix F). A noncriminal justice agency must notify applicants of their privacy rights by providing applicants with a copy of the Noncriminal Justice Applicant's Privacy Rights document (Appendix G). Information is also available in the Privacy Act Statement (Appendix H).

Right to Review

Pursuant to La. Revised Statute 15:588, an individual can obtain a certified copy of his/her personal criminal history record as maintained by the LSP Bureau. Individuals must submit a "Right to Review Authorization Form" and a "Right to Review Disclosure Form" along with fingerprints and the appropriate fees to the LSP Bureau (for forms and information go to: http://www.lsp.org/technical.html#criminal). Individuals can use this record to identify, if applicable, the date of an arrest, the identity of an arresting agency, and disposition information. This criminal history record may only be given to the individual, his authorized representative or his attorney.

FBI Identity History Summary checks:

The U.S. Department of Justice Order 556-73, also known as Departmental Order, establishes rules and regulations for individuals to obtain a copy of their Identity History Summary for review or proof that one does not exist. The individual may submit fingerprints, an Applicant Information Form, and payment directly to the FBI according to the procedures in Title 28 Code of Federal Regulations 16.34.

FBI website for information about record review and challenge:
https://www.fbi.gov/services/cjis/identity-history-summary-checks

Security of Criminal History Record Information

Noncriminal justice agencies must have written policies and procedures regarding access, use, dissemination, and disposal of CHRI. These policies and procedures must be made available to LSP Bureau personnel or the CJIS Information Security Officer (ISO) upon request.

CSP 5.1.1.1 Information Handling

Noncriminal justice agencies must have written policies and procedures regarding access, use and handling, and destruction of CHRI. Procedures for handling and storage of information shall be established to protect that information from unauthorized disclosure, alteration or misuse. Using the requirements in the CJIS Security Policy as a starting point, the procedures shall apply to the handling, processing, storing, and communication of CJI. These procedures apply to the exchange of CJI no matter the form of exchange.

The agency must have a process which ensures that CHRI is only used for the purpose for which it is requested.

The agency must have processes in place for the proper access and handling of CHRI. The agency policy should include:

- Defining who is authorized to access CHRI.
- Restricting access to only Authorized Personnel.
- Handling rules.

- Proper security of CHRI from receipt through destruction.
- Communication of rules to appropriate personnel.
- Communication among Authorized Personnel.
- Communication with the applicant concerning CHRI.
- Retention procedures.
- Destruction procedures

The agency must have processes in place to prevent the unauthorized disclosure of CHRI. The agency policy to prevent unauthorized disclosure should include:

- Access-limited storage.
- Not leaving CHRI unattended when it is not physically secured.
- Revocation of access privileges for terminated employees or those removed from Authorized Personnel List.

The agency must have a formal disciplinary process in place for misuse of CHRI. If the agency has a general misconduct or disciplinary policy, the agency would need to demonstrate how this policy would be applied in the event of a misuse situation.

If applicable, the agency must have processes in place governing the electronic storage of CHRI. This includes:

- Monitoring and restricting access to databases containing CHRI.
- Physical/technical safeguards to protect the access and integrity of the CHRI.
- Reporting, response, and handling capability for information security incidents.

CSP 5.8.4 Disposal of CHRI

Physical media shall be securely disposed of when no longer required, using formal procedures. Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information being compromised by unauthorized individuals. Physical media shall be destroyed by shredding or incineration. Agencies shall ensure disposal or destruction is witnessed or carried out by authorized personnel.

The agency shall sanitize, by overwriting at least three times or degaussing 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. The agencies must have these procedures written in the agencies policy.

CSP 5.9 Physical Security

Agencies are required to establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity. Agencies must have these procedures written in their agency policy. This includes maintaining the criminal history record information in a secure location that is not readily accessible to individuals not authorized to see it.

Physical Security includes:

- Protection of information subject to confidentiality.
- Limitation of visitor access to controlled areas.

- Positioning of computer and system devices (lap tops, cellular phones, I-pads, or any kind of hand held devices used to access, process, or store CHRI media) in such a way that prevents unauthorized personnel gaining physical or visual access.
- Locking of rooms, areas, or storage containers where CHRI media is accessed, processed and/or stored.
- CHRI shall not be stored in an individual's personnel file.

Electronic Security includes:

- Protection of information subject to confidentiality via state and/or federal statute or regulation.
- Password use and management.
- Protection from viruses, worms, Trojan horses and other malicious code.
- Appropriate use and management of e-mail, spam and attachments.
- Appropriate web use.
- Use of encryption; for transmission and storage of sensitive/confidential information through electronic means.

IT personnel's responsibility to install:

- Protection from viruses, worms, Trojan horses, and other malicious code through scheduled electronic scanning and definition updates.
- Provide scheduled data backup and storage.
- Provide timely application of system patches as part of configuration management (i.e. Windows updates should be performed monthly).
- Provide physical and electronic access control measures.
- Provide protection measures for agency Network infrastructure (i.e. Perimeter firewalls, intrusion prevention, web content filtering, email spam and virus filtering).

Maintenance (Retention) Of Criminal History Record Information

Criminal history record information may be retained in hard copy format and electronic format. It needs to be retained only for the length of time it is needed to make eligibility determinations and allow adequate time for an applicant to complete or challenge the accuracy of the information in the record. Pursuant to the CJIS Security Policy 4.2.4, the records shall be stored for extended periods of time only when they are key elements for the integrity and/or utility of case files. Therefore, if it is not an agency requirement, the hard copy record information shall be destroyed.

CSP 5.8 Policy Area 8: Media Protection

Media protection policy and procedures shall be documented and implemented to ensure that access to digital and physical media in all forms is restricted to authorized individuals. Procedures shall be defined for securely handling, transporting and storing media.

5.8.1 Media Storage and Access

The agency shall securely store digital and physical media within physically secure locations or controlled areas. The agency shall restrict access to digital and physical media to authorized individuals. If physical and personnel restrictions are not feasible then the data shall be encrypted per Section 5.10.1.2.

5.8.2 Media Transport

The agency shall protect and control digital and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel.

5.8.2.1 Digital Media during Transport

Controls shall be in place to protect digital media containing CJI while in transport (physically moved from one location to another) to help prevent compromise of the data. Encryption, as defined in Section 5.10.1.2 of this Policy, is the optimal control during transport; however, if encryption of the data isn't possible then each agency shall institute physical controls to ensure the security of the data.

5.8.2.2 Physical Media in Transit

The controls and security measures in this document also apply to CJI in physical (printed documents, printed imagery, etc.) form. Physical media shall be protected at the same level as the information would be protected in electronic form.

5.8.3 Digital Media Sanitization and Disposal

The agency shall sanitize, that is, overwrite at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable digital media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel.

5.8.4 Disposal of Physical Media

Physical media shall be securely disposed of when no longer required, using formal procedures. Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information compromised by unauthorized individuals. Physical media shall be destroyed by shredding or incineration. Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel.

5.8.5 References/Citations/Directives

A list of all of the references used in the FBI CJIS Security Policy are found in that document's Appendix I and may contain additional sources that apply to this section (Appendix I).

CSP 5.9.2 Controlled Area

If an agency cannot meet all of the controls required for establishing a physically secure location, but has an operational need to access or store CJI, the agency shall designate an area, a room, or a storage container, as a controlled area for the purpose of day-to-day CJI access or storage. The agency shall, at a minimum:

- Limit access to the controlled area during CJI processing times to only those personnel authorized by the agency to access or view CJI.
- Lock the area, room, or storage container when unattended.
- Position information system devices and documents containing CJI in such a way as to prevent unauthorized individuals from access and view.

- Follow the encryption requirements found in Section 5.10.1.2 for electronic storage (i.e. data "at rest") of CJI.

CSP 5.3 Incident Response

To ensure protection of CJI, agencies shall:

- Establish operational incident handling procedures that include adequate preparation, detection, analysis, containment, recovery, and user response activities.
- Track, document, and report incidents to appropriate agency officials and/or authorities..

Each Agency shall identify a Local Agency Security Officer (LASO). The LASO is the point of contact on security related issues for their agency.

LASOs are responsible for instituting the CJIS Information Security Officer (ISO) incident response reporting procedures at their agency as needed. The Agency LASO shall:

- Identify who is using the CSA approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.
- Identify and document how the equipment is connected to the state system.
- Ensure that personnel security screening procedures are being followed as stated in this Policy.
- Ensure the approved and appropriate security measures are in place and working as expected.
- Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.

OTS Information Security Policy – Incident Management

The Louisiana Division of Administration (DOA) Office of Technology Services (OTS) Information Security Policy (OTS ISP) outlines the Incident Management Program (pgs. 39-44). This program clearly establishes the phases, actions, responsibilities and documentation requirements for handling all incidents. This section of the Information Security Policy applies to any and all efforts related to the detection, action, documentation and communication of an incident (Appendix J).

CSP 5.7 Policy Area 7: Configuration Management

CSP 5.7.1 Access Restrictions for Changes

Planned or unplanned changes to hardware, software, and/or firmware components of the information system can have significant effects on the overall security of the system. The goal is to allow only qualified and authorized individuals access to information system components for purposes of initiating changes, including upgrades, and modifications. The essential premise of the CJIS Security Policy is to provide appropriate controls to protect the full lifecycle of CHRI, whether at rest or in transit. The CJIS Security Policy provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. This Policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information.

CSP 5.7.1.2 Network Diagram

The agency shall ensure that a complete topological drawing depicting the interconnectivity of the agency network, to criminal justice information, systems and services is maintained in a current status.

The network topological drawing shall include the following:

- All communications paths, circuits, and other components used for the interconnection, beginning with the agency-owned system(s) and traversing through all interconnected systems to the agency end-point.
- The logical location of all components (e.g., firewalls, routers, switches, hubs, servers, encryption devices, and computer workstations). Individual workstations (clients) do not have to be shown; the number of clients is sufficient.
- "For Official Use Only" (FOUO) markings.
- The agency name and date (day, month, and year) drawing was created or updated.

CSP Policy Area 10: System and Communications Protection and Information Integrity

Encryption

The OTS Information Security Policy (pgs. 33-34) defines acceptable encryption practices in order to ensure CHRI is adequately protected and compliant with regulatory requirements. It is imperative that only authorized data encryption methods be used. This policy section documents the standards for storing and transmitting Confidential and Restricted Data, whether managed by an Agency, OTS, or a third party. This section also provides policies for the management of encryption keys (Appendix J).

This section does not intend to conflict with any Federal, State, or local law for use of encryption technologies outside of the United States.

Encryption Standards

Confidential and Restricted Data that will traverse the internet, public or untrusted networks, or transmitted wirelessly shall be encrypted in accordance with Encryption Requirements. In addition, Confidential and Restricted Data stored on laptops and other portable devices, shall be encrypted in accordance with Encryption Requirements. In the event technical or operational limitations are identified and cannot be addressed, which prevent the required use of encryption for laptops and other mobile devices, the Agency shall complete the Exception Request process.

The use of proprietary data encryption methods for Confidential and Restricted Data protection is strictly prohibited.

Encryption Key Management

Encryption keys must be generated, accessed, distributed and stored in a controlled and secured manner as specifically required below.

Key Access - Access to encryption keys used to encrypt and decrypt Restricted Data must strictly comply with Access and Identity Management. The Chief Information Security Officer (CISO) is the Data Owner of encryption keys. The CISO shall perform periodic reviews of the users with access to encryption keys.

Split Knowledge and Dual Control - When required, a minimum of two encryption key users are required to perform any key action (such as key generation or loading the key). Additionally, no single user with encryption key access shall know or have access to all pieces of a data encryption key.

Key Generation - Creation of encryption keys must be accomplished using a random or pseudo-random number generation algorithm. Generating encryption keys must be accomplished by a minimum of two authorized users.

Key Storage - All encryption keys must be encrypted and stored in a secure location as determined by CISO. Key-encrypting keys must be stored separately from data-encrypting keys. Clear-text backups of encryption key components must be stored separately in tamper-evident storage in a secure location. Only users with access to encryption keys shall be authorized to retrieve key components from secure storage or distribute encryption keys.

Key Changes and Destruction - An encryption key change is the process of generating a new key, decrypting the current production data and re-encrypting the Confidential and Restricted Data with the new encryption key.

Training

All persons directly associated with accessing, maintaining, processing, dissemination or destruction of CHRI shall be trained. The training shall provide employees with a working knowledge of federal and state regulations and laws governing the security and processing of criminal history information. The NAC is responsible for ensuring agency personnel receive such training within six (6) months of employment or job assignment and every two (2) years thereafter.

Agencies are responsible for complying with mandatory training requirements. Per the CJIS Security Policy 5.2, all agency personnel who view or handle CHRI must complete CJIS Security Awareness training as well as any agency-specific training on CHRI security and handling based on the agency's required policies/procedures.

CSP 5.2 Security Awareness Training

Training must be completed within six (6) months of initial assignment and requires recertification every two (2) years for noncriminal justice agency personnel. If the noncriminal justice agency has engaged in a Security and Management Control Outsourcing Standard for Non-Channelers, vendor personnel must recertify annually (yearly). All personnel who are required to complete Security Awareness Training must sign an Acknowledgement Statement of Misuse acknowledging the notification of the penalties for misuse of CHRI (Appendix K).

The LSP Bureau will provide training or instruction on fingerprint handling and submission for all agencies accessing CHRI. The CJIS Security Training is located at www.cjisonline.com. The agency's NAC is responsible for setting up user accounts for all personnel who must be certified.

There are 4 Levels of CJIS Security Training:

Level 1 Security Awareness Training (CSP 5.2.1.1)

At a minimum, the following topics shall be addressed as baseline security awareness training for personnel with unescorted access to a physically secure location (This level is designed for people who have access to a secure area but are not authorized to use FBI Criminal History Results. Examples: Custodial staff, maintenance staff.)

Training must address:

- Individual responsibilities and expected behavior with regard to being in the vicinity of CJI usage and/or terminals.
- Implications of noncompliance.
- Incident response (Identify points of contact and individual actions).
- Visitor control and physical access to spaces—discuss applicable physical security policy and procedures, e.g., challenge strangers, report unusual activity, etc.

Level 2 Security Awareness Training (CSP 5.2.1.2)

In addition to 5.2.1.1 above, the following topics, at a minimum, shall be addressed as baseline security awareness training for all authorized personnel with access to CJI. Examples: Personnel that view, handle, or have knowledge or access to storage locations where CHRI is stored.

Training must address:

- Media protection.
- Protect information subject to confidentiality concerns — hardcopy through destruction.
- Proper handling and marking of CJI.
- Threats, vulnerabilities, and risks associated with handling of CJI.
- Social engineering.
- Dissemination and destruction.

Level 3 Security Awareness Training (CSP 5.2.1.3)

In addition to 5.2.1.1 and 5.2.1.2 above, the following topics, at a minimum, shall be addressed as baseline security awareness training for all authorized personnel with both physical and logical access to CJI. Examples: This Level is designed for personnel who typically have access to query, enter, or modify Criminal History Information data in an electronic format.

Training must address:

- Rules that describe responsibilities and expected behavior with regard to information system usage.
- Password usage and management—including creation, frequency of changes, and protection.
- Protection from viruses, worms, Trojan horses, and other malicious code.
- Unknown e-mail/attachments.
- Web usage—allowed versus prohibited; monitoring of user activity.
- Spam.
- Physical Security—increases in risks to systems and data.
- Handheld device security issues—address both physical and wireless security issues.
- Use of encryption and the transmission of sensitive/confidential information over the Internet—address agency policy, procedures, and technical contact for assistance.
- Laptop security—address both physical and information security issues.
- Personally owned equipment and software—state whether allowed or not (e.g. copyrights).
- Access control issues—address least privilege and separation of duties.
- Individual accountability—explain what this means in the agency.
- Use of acknowledgement statements—passwords, access to systems and data, personal use and gain.

- Desktop security—discuss use of screensavers, restricting visitors' view of information on screen (mitigating "shoulder surfing"), battery backup devices, allowed access to systems.
- Protect information subject to confidentiality concerns—in systems, archived, on backup media, and until destroyed.
- Threats, vulnerabilities, and risks associated with accessing CJIS Service systems and services.

Level 4 Security Awareness Training (CSP 5.2.1.4)

In addition to CSP 5.2.1.1, 5.2.1.2, and 5.1.2.3 above, the following topics at a minimum shall be addressed as baseline security awareness training for all Information Technology personnel. Examples: system administrators, security administrators, network administrators, etc.

Training must address:

- Protection from viruses, worms, Trojan horses, and other malicious code—scanning, updating definitions.
- Data backup and storage—centralized or decentralized approach.
- Timely application of system patches—part of configuration management.
- Access control measures.
- Network infrastructure protection measures

Authorized Personnel training must be logged on the NCJA Training Documentation Form and the documentation must be available for inspection by auditors (Appendix L).

Outsourcing

The CJIS Security Policy 5.1.1.8, Outsourcing Standards for Non-Channelers, requires that an authorized recipient's use of a third party to administer noncriminal administrative functions, such as making fitness recommendations, obtaining missing dispositions, archival and off-site storage of fingerprint submissions and corresponding criminal history record results, or the submission of fingerprints and the receipt of corresponding criminal history records, must meet all requirements set forth in the Security and Management Control Outsourcing Standard (Appendix M) and be approved by the LSP Bureau prior to engaging in such an agreement or contract. To ensure agencies follow these minimum standards, the Outsourcing Standard provides that contracts and agreements authorized by this rule "shall incorporate by reference a Security and Management Control Outsourcing Standard."

Audit

CJIS Security Policy 5.11 Formal Audits authorize the FBI CJIS Division to conduct security audits of Louisiana State Police, the state's CJIS System Agency (CSA), and the LSP Bureau's networks and systems, once every three (3) years as a minimum, to assess agency compliance with the CJIS Security Policy. To assess noncriminal justice agencies compliance with the CJIS Security Policy, the LSP Bureau shall:

- At a minimum, triennially audit all CJAs and NCJAs which have direct access to the state system in order to ensure compliance with applicable statutes, regulations and policies.
- In coordination with the LSP Bureau, establish a process to periodically audit all NCJAs, with access to CJI, in order to ensure compliance with applicable statutes, regulations and policies.

- Have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.
- Have the authority, on behalf of another CSA, to conduct a CSP compliance audit of contractor facilities and provide the results to the requesting CSA. If a subsequent CSA requests an audit of the same contractor facility, the CSA may provide the results of the previous audit unless otherwise notified by the requesting CSA that a new audit be performed.

In other words, Noncriminal Justice Agencies (NCJA) that are authorized to receive CHRI for noncriminal justice purposes are subject to audit to ensure compliance with state and federal rules regarding fingerprint submissions and CHRI use. The NCJA may be audited every three years in order to assess compliance with state and federal policies and regulations. The NCJA may also be audited as part of triennial FBI audits of the LSP Bureau.

Appendices

Appendix A FBI CJIS Security Policy

https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center

Appendix B Civil Agency User Agreement

http://www.lsp.org/pdf/Civil_Agency_User_Agreement.pdf

Appendix C Local Agency Security Officer (LASO) form

http://www.lsp.org/pdf/Local_Agency_Security_Officer_Appointment.pdf

Appendix D Security Incident Reporting form

http://www.lsp.org/pdf/Security_Incident_Reporting_Form.pdf

Appendix E Noncriminal Agency Coordinator (NAC) form

http://www.lsp.org/pdf/Noncriminal_Agency_Coordinator.pdf

Appendix F Agency Privacy Requirements for Noncriminal Justice Applicants

http://www.lsp.org/pdf/Agency_Privacy_Requirements_NJA.pdf

Appendix G Noncriminal Justice Applicant's Privacy Rights

http://www.lsp.org/pdf/Noncriminal_Justice_Applicants_Privacy_Rights.pdf

Appendix H Privacy Act Statement

http://www.lsp.org/pdf/Privacy_Act_Statement.pdf

Appendix I CJIS Security Policy Appendix I References

http://www.lsp.org/pdf/CJIS_Security_Policy_Appendix_I_References.pdf

Appendix J OTS Information Security Policy

http://www.lsp.org/pdf/OTS_Information_Security_Policy.pdf

Appendix K Statement of Misuse

http://www.lsp.org/pdf/Statement_of_Misuse.pdf

Appendix L NCJA Training Documentation form

http://www.lsp.org/pdf/NCJA_Training_Documentation_Form.pdf

Appendix M Security and Management Control Outsourcing Standard for Non-channelers

https://www.fbi.gov/file-repository/security-and-management-control-outsourcing-standard-for-non-channelers-2.pdf/view