Guide for Non-Criminal Justice Agencies

Version 1.1

July 23, 2024

Prepared By:

Florida Department of Law Enforcement
Criminal Justice Information Services Division
Criminal History Services Section

Introduction

This guide was created to assist non-criminal justice agencies (to include entities and organizations) that submit fingerprints and receive criminal history record information for non-criminal 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 non-criminal 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 non-criminal 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 Federal Bureau of Investigation's (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 Florida Department of Law Enforcement (FDLE) has established and maintains intrastate systems for the collection, compilation, and dissemination of state criminal history records and information in accordance with subsection 943.05(2), Florida Statutes (F.S.), and is authorized and does, in fact, participate in federal and interstate criminal history records systems, pursuant to s. 943.051, F.S.

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, informations, 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] to any person or agency that would not be eligible to receive the information itself."

CHRI is also described by the FBI CJIS Security Policy 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 criminal history record 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.

FBI Criminal Justice Information Services (CJIS) Security Policy

The FBI Criminal Justice Information Services (CJIS) Security Policy (CJISSECPOL) provides 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 CJISSECPOL integrates presidential directives, federal laws, FBI directives, and the criminal justice community's Advisory Policy Board (APB) decisions, along with nationally-recognized guidance from the National Institute of Standards and Technology (NIST).

As use of criminal history record information for non-criminal justice purposes continues to expand, the CJISSECPOL becomes increasingly important in the secure exchange of criminal justice records. The CJISSECPOL 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 non-criminal justice communities.

Non-Criminal Justice Agency User Agreement

Pursuant to the FBI CJIS Security Policy (Section 5.1.1.6), 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 Florida Department of Law Enforcement (FDLE). The User Agreement and the FBI CJIS Security Policy contain 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. Non-criminal justice agencies are prohibited from using criminal history record information for any purpose other than that for which it was requested.

Sanctions/Penalties: Either FDLE or the User may suspend the performance of services under this agreement when, in the reasonable estimation of FDLE or the User, the other party has breached any material term of the agreement. Furthermore, upon FDLE becoming aware of violations of this agreement which jeopardize Florida's access to national criminal history information, FDLE shall have the option of suspending services under this agreement, pending resolution of the problem. The violation of any material term of this agreement or of any substantive requirement or limitation imposed by the federal or state statutes, regulations, or rules referred to in this agreement shall be deemed a breach of a material term of the agreement. This agreement is also terminable upon the same grounds and upon the occurrence or non-occurrence of such events that operate to suspend, annul, or void any other long-term contract entered into by a state agency.

Local Agency Security Officer (LASO): Pursuant to the FBI CJIS Security Policy (Section 3.2.9), the User Agreement requires the appointment of a LASO to function as the point of contact with regard to security and audit-related issues, as well as coordinate FBI CJIS Security Policy compliance for the non-criminal justice agency.

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 Florida 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 CHRI can be a misdemeanor or felony, depending on the circumstances.

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 non-criminal justice purpose. These rights are detailed in the *Agency Privacy Requirements for Noncriminal Justice Applicants* document. A non-criminal justice agency must notify

applicants of their privacy rights by providing applicants with the *Privacy Act Statement* and *Noncriminal Justice Applicant's Privacy Rights* document prior to or at the time of fingerprinting. This process must be incorporated into agency policy and be an auditable process—for reference, a *Sample National Rap Back Policy* and *Applicant Waiver Agreement and Statement Form* are available on the CJIS Launch Pad's *Informational Documents* page.

Right to Review

Pursuant to s. 943.056, F.S., and Florida Administrative Code Rule 11C-8.001, an individual can obtain a copy of his/her personal criminal history record as maintained by the Florida Department of Law Enforcement (FDLE). Individuals may perform a fee-based search or initiate a Personal Review application through FDLE's website.

If the individual believes the national criminal history record information is in error, a personal review request can be made to the Federal Bureau of Investigation (FBI), pursuant to 28 CFR Sections 16.30-16.34. Individuals may initiate an Identity History Summary Check through the FBI's website.

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/her authorized representative, or his/her attorney.

FBI CJIS Security Policy and Procedure Requirements:

Non-criminal justice agencies must have written policies and procedures regarding access, use, dissemination, storage, physical security, transmission, and disposal of CHRI/CJI. These policies and procedures must be made available to Florida Department of Law Enforcement (FDLE) personnel or the CJIS Information Security Officer (ISO) upon request.

Information Handling

Non-criminal justice agencies must have written policies and procedures regarding access, use, handling, and destruction of CHRI. Procedures for the handling and storage of information shall be established to protect that information from unauthorized disclosure, alteration, or misuse. Using the requirements in the FBI 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 CJI 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 CJI. The agency policy should include:

- Defining who is authorized to access CJI
- Restricting access to only Authorized Personnel
- Current agency procedures for handling CJI
- Security of CJI from receipt through destruction
- Retention policies
- Destruction procedures

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

- Security controls in place for the secure storage of CJI
- Procedures for how to secure CJI when leaving an area unattended

- Revocation of access privileges and accounts for terminated employees or those removed from positions that require access to CJI

The agency must have a formal disciplinary process in place for misuse of CJI.

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

- Monitoring and restricting access to servers, systems, and/or applications containing CJI
- Physical/technical safeguards to protect access and integrity of CJI
- Reviewing logs for servers, systems, and/or applications containing CJI
- Reporting, response, and handling capability for information security incidents

Physical Security

Agencies are required to establish appropriate administrative, technical, and physical safeguards to ensure 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 unauthorized individuals.

Physical Security includes:

- Protection of information subject to confidentiality
- Marking digital and non-digital media that contains CJI
- Access controls in place for visitors of areas where CJI is accessed, processed, or stored
- Positioning of computer and system devices used to access, process, or store CJI in such a way that prevents unauthorized personnel from shoulder surfing
- Locking of rooms, areas, or storage containers where CJI is accessed, processed, and/or stored
- Ensuring that signs are posted to mark where physical access is limited based on security requirements

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 control of e-mail, spam, and attachments
- Appropriate web use
- Use of encryption for transmission and storage of CJI through electronic means, as well as for data at rest outside of the boundary of the physically-secure location

Information Technology support personnel's responsibility:

- 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
- Provide physical and electronic access control measures
- Provide protection measures for agency Network infrastructure

Retention of Criminal Justice Information

Criminal justice information may be retained in hard copy format and electronic format. It needs to be retained only for the length of time as required by Florida retention statutes. The agency must allow adequate time for an applicant to complete or challenge the accuracy of the information in the record.

Policy Area 5.8: Media Protection

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

Media Storage and Access

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

Media Transport

The agency shall protect and control digital and non-digital media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel. Non-digital media can be carried in secure containers such as folders, envelopes, briefcases, etc., while digital media must be encrypted when transmitted outside of the physically-secure location.

Digital Media Sanitization and Disposal

The agency shall sanitize, that is, overwrite at least three (3) times or degauss digital media prior to disposalor 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.

Disposal of Non-digital Media

Non-digital 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. Non-digital media shall be destroyed by cross-cut shredding or incineration. Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel.

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 CJIS Systems Agency (CSA)-approved hardware, software, and firmware and ensure nounauthorized 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
- 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

Configuration Management

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 FBI CJIS Security Policy is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The FBI 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.

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

System and Communications Protection and Information Integrity

Information Flow Enforcement

The network infrastructure shall control the flow of information between interconnected systems. Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. In other words, controlling how data moves from one place to the next in a secure manner.

Boundary protection devices must be enabled on the agency's network that contains CJI. These devices must control access to networks that process CJI, as well as monitor and control communications throughout the entire network.

Encryption Standards

CJI that will traverse the internet, public or untrusted networks, or that is transmitted wirelessly must be encrypted in accordance with Encryption Requirements outlined in the FBI CJIS Security Policy. Any wireless devices that accesses CJI must have the hard drive encrypted. The encryption levels must meet NIST standards of Federal Information Processing Standard (FIPS) 140-2 certification.

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 Local Agency Security Officer (LASO) is responsible for ensuring agency personnel receive such training within six (6) months of employment or job assignment prior to access and annually thereafter.

Agencies are responsible for complying with mandatory training requirements. Pursuant to the FBI CJIS Security Policy (Section 5.2), all agency personnel who have access to CJI within six (6) months of employment or job assignment prior to access and annually thereafter 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.

CJISSECPOL 5.2 Awareness and Training (AT)

Training must be completed as part of initial training for new users, prior to accessing CJI and annually thereafter. If the non-criminal justice agency has engaged in a Security and Management Control Outsourcing Standard for Non-Channelers, vendor personnel must also recertify annually.

The agency will be responsible for ensuring that agency provided literacy training and awareness occurs for all system users, including managers, senior executives, and contractors as part of initial training and when required by system changes or within thirty (30) days of any security event for all individuals involved in the event. The training must be updated annually and incorporate lessons learned from internal or external security incidents or breaches. The training must include insider threat training along with social engineering and mining. All agency personnel must take the training on an annual basis.

The FBI CJIS Security Policy also requires agencies to provide role-based training to all agency personnel. FDLE provides training and instruction on fingerprint handling and submission for all agencies accessing CHRI; CJIS Role-Based Training is located within the CJIS Online system (https://www.cjisonline.com). The agency must have a point of contact who is responsible for setting up and maintaining user accounts for all personnel who must be certified.

There are four (4) levels of Role-Based Training:

Basic Role: For all individuals with unescorted access to a physically-secure location.

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 agency personnel who have access to a secure area, but are not authorized to access FBI criminal history information).

Training must address:

- Access, Use, and Dissemination of Criminal History Record Information (CHRI), National Crime Information Center (NCIC) Restricted Files Information, and NCIC Non-Restricted Files Information Penalties
- Reporting Security Events
- Incident Response Training
- System Use Notification
- Physical Access Authorizations

- Physical Access Control
- Monitoring Physical Access
- Visitor Control
- Personnel Sanctions

General Role: A user, but not a process, who is authorized to use an information system.

In addition to the *Basic Role* topics above, the following topics, at a minimum, shall be addressed as baseline security awareness training for all authorized personnel with access to CJI.

Training must address:

- Criminal Justice Information
- Proper Access, Use, and Dissemination of NCIC Non-Restricted Files Information
- Personally Identifiable Information
- Information Handling
- Media Storage
- Media Access
- Audit Monitoring, Analysis, and Reporting
- Access Enforcement
- Least Privilege
- System Access Control
- Access Control Criteria
- System Use Notification
- Session Lock
- Personally Owned Information Systems
- Password
- Access Control for Display Medium
- Encryption
- Malicious Code Protection
- Spam and Spyware Protection
- Cellular Devices
- Mobile Device Management
- Wireless Device Risk Mitigations
- Wireless Device Malicious Code Protection
- Literacy Training and Awareness/Social Engineering and Mining
- Identification and Authentication (Organizational Users)
- Media Protection

Privileged Role: A user that is authorized (and, therefore, trusted) to perform security-relevant functions that general users are not authorized to perform.

In addition to AT-3 (d) (1) and (2) above, include the following topics:

a. Access Control
b. System and Communications Protection and Information Integrity
c. Patch Management
d. Data backup and storage—centralized or decentralized approach
e. Most recent changes to the FBI CJIS Security Policy

Organizational Personnel with Security Responsibilities (Security Role): Personnel with the responsibility to ensure the confidentiality, integrity, and availability of CJI and the

implementation of technology in a manner compliant with the FBI CJIS Security Policy.

In addition to AT-3 (d) (1), (2), and (3) above, include the following topics:

Training must address:

- Local Agency Security Officer (LASO) Role
- Authorized Recipient Security Officer Role
- Additional state/local/tribal/federal agency roles and responsibilities
- Summary of audit findings from previous state audits of local agencies
- Findings from the last FBI CJIS Division audit.

Outsourcing

The FBI CJIS Security Policy (Section 5.1.1.8), Outsourcing Standards for Non-Channelers, requires that Contractors designated to perform non-criminal justice ancillary functions on behalf of a NCJA (public) or NCJA (private) for non-criminal justice functions shall be eligible for access to CJI.

Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. All contractors accessing CJI shall be subject to the terms and conditions described in the Compact Council Outsourcing Standard for Non-Channelers. Contractors leveraging CJI to perform civil functions on behalf of an Authorized Recipient shall meet the same training and certification criteria required by governmental agencies performing a similar function and shall be subject to the same extent of audit review as are local user agencies.

Audit

The FBI CJIS Security Policy (Section 5.11), Formal Audits, authorize the FBI's CJIS Division to conduct security audits of the Florida Department of Law Enforcement (FDLE), the state's CJIS System Agency (CSA), to include networks and systems, once every three (3) years as a minimum to assess agency compliance with the FBI CJIS Security Policy.

To assess non-criminal justice agencies compliance with the FBI CJIS Security Policy, FDLE shall:

- At a minimum, triennially audit all Criminal Justice Agencies (CJAs) and Non-Criminal Justice Agencies (NCJAs) which have 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 CJIS 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, NCJAs that are authorized to receive CJI for non-criminal justice purposes are subject to audit to ensure compliance with state and federal rules regarding fingerprint submissions and CJI use. The NCJA may be audited every three (3) 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 FDLE.

Need Assistance?

Agencies/entities may refer to the *Noncriminal Justice CJIS Compliance and Training* section of FDLE's website and the CJIS Launch Pad for additional information and resources.

Agencies/entities needing additional assistance may contact FDLE's Criminal History Services Section (CHS) during business hours—Monday through Friday, 9:00 AM – 4:00 PM (EST) (excluding holidays)—by telephone at (850) 410-8161 (please remain on the line through the telephone prompts) or by e-mail at ApplicantChecks@fdle.state.fl.us.