Louisiana Noncriminal Justice Agency Onboarding Packet

Contents

Acronym Glossary

Acronym	Term
CHRI	Criminal History Record Information
CJI	Criminal Justice Information
CJIS	Criminal Justice Information Services
CJISSECPOL	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	Non-Criminal Agency Coordinator
NCJA	Non-Criminal 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 non-criminal justice agencies (NCJAs) that submit fingerprints and receive criminal history record information (CHRI) for non-criminal justice purposes pursuant to authorizations allowed by state and federal law. Included in this guide are forms and documents that must be completed to be onboarded as a NCJA as well as information regarding the responsibilities of accessing and maintaining CHRI data.

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 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.

Criminal History Record Information Databases

The FBI maintains an automated database, Next Generation Identification (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 BCII) is the state's designated repository that stores criminal history record information (CHRI) in the Louisiana Computerized Criminal History (LACCH) database.

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 in the FBI CJIS Security Policy, Section 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 database 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.

FBI Criminal Justice Information Services (CJIS) Security Policy

The FBI's Criminal Justice Information Services 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, non-criminal 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's decisions, along with nationally recognized guidance from the National Institute of Standards and Technology. As use of criminal history record information (CHRI) for non-criminal 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 non-criminal justice communities. A copy of the CJIS Security Policy can be found in Appendix A.

A non-criminal justice agency (NJCA) needs to be aware of the CJIS Security Policy as the criminal history record information (CHRI) that results from a fingerprint-based background check is considered criminal justice information. Therefore, the CJIS Security Policy provides the requirements and standards for ensuring the security and confidentiality of this information.

I have read and acknowledged the above information. _____

Initials

What is Criminal History Record Information (CHRI)?

When an agency submits fingerprints to the LSP Bureau for a background check, the result of that check is criminal history record information (CHRI). A non-criminal justice agency receiving CHRI is responsible for ensuring the security and confidentiality of the record itself and all references to the contents therein.

Criminal history record information, received from the LSP Bureau, does not include driver history records or arrests in which the offender was issued a summons.

I have read and acknowledged the above information. _____

Initials

Access to Criminal History Record Information (CHRI)

A non-criminal justice agency (NCJA) can only receive CHRI if there is a statute in place providing the authority to do so. The statutory authority will either specify that the NCJA can receive state and federal results (from LACCH and NGI, respectively) from fingerprint-based background checks, or receive state-only results. A NCJA cannot receive the results of background checks without a statutory authority. Each authority within the state of Louisiana has been assigned an Applicant Type Code by the LSP Bureau. The LSP Bureau will confirm or provide the statutory authority and correlated Applicant Type Code if unknown to the NCJA.

ORIs/Account Numbers

Once the statutory authority is established, the LSP Bureau will assign a NCJA a nine-character account number called an ORI. The LSP Bureau will notify the NCJA of their ORI upon execution of the Civil Agency User Agreement. The ORI is a critical component of tracking the dissemination of CHRI between the LSP Bureau and the NCJA.

When a statute authorizes a NCJA to receive state and federal CHRI, the LSP Bureau will assign an ORI that begins with LA, followed by 7 letters and numbers. When a statute authorizes state only CHRI, the LSP Bureau will assign an ORI that begins with CRU, followed by 6 numbers.

The NCJA is required to include the ORI and Applicant Type Code with every fingerprint submission. These are included in the Background Check Authorization Form (Appendix K), provided to a NCJA by the LSP Bureau. This form is to be used in conjunction with the appropriate Disclosure Form when requesting background checks with fingerprint cards. The LAPS Authorization Form (Appendix L) is for agencies that use the LAPS program.

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 (CHRI) for non-criminal justice purposes.

28 C.F.R. § 20.31 allows the FBI to collect fees for non-criminal 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 non-criminal 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 money to them monthly.

Louisiana Applicant Processing System (LAPS)

The Louisiana Applicant Processing System (LAPS) is a new program implemented by the Louisiana State Police (LSP) in 2023 to provide fast and efficient criminal history background check results to non-criminal justice agencies. The LAPS program is a digital fingerprint capture system utilizing Idemia's Identogo network of enrollment centers located around the state of Louisiana. The Identogo network allows applicants to submit fingerprints in their local area of domicile, eliminating the need to travel long distances to be fingerprinted or the need to submit fingerprint cards to the Louisiana State Police's Bureau of Identification and Information (LSP BCII) to obtain a criminal history report. Applicants can schedule their own appointments at a time and place convenient for them. Requesting agencies then log into a web portal to obtain the criminal history background check results for their applicants. Criminal History Record Information (CHRI) remains securely stored in the LAPS program's web portal in compliance with CJIS Security policies, eliminating the need for individual

agencies to have to store CHRI locally. Background check results are now available to non-criminal justice agencies in a matter of hours after a fingerprint submission rather than days or weeks. Your agency must work with the LSP BCII directly to receive a LAPS account.

I have read and acknowledged the above information. _____

Initials

Civil Agency User Agreement

Pursuant to the CJIS Security Policy (CJISSECPOL), Section 5.1.1.2 "State and Federal 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, the non-criminal justice agency (NCJA) requesting the results of the background check, and the LSP Bureau. This agreement authorizes the LSP Bureau to share CHRI with the NCJA. Without a User Agreement in place, the LSP Bureau does not have the authority to disseminate CHRI.

A Civil Agency User Agreement shall be in place prior to non-criminal justice agencies receiving CHRI. If a NCJA does not have a User Agreement, or if the signatory roles have changed since the agreement was executed, the agency must contact the LSP Bureau at *LSP.BCII.NCJA@la.gov* to execute a new agreement.

The User Agreement contains Terms and Conditions which include the following:

Authority and Purpose: The User Agreement identifies the requesting Agency, the purpose for which criminal history record information is requested, and the specific statutory authority 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: 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 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 of the receiving Agency.**

Misuse of CHRI: The exchange of CHRI is subject to immediate cancellation if dissemination is made outside of 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 CHRI can be a misdemeanor or felony depending on the circumstances.

The User Agreement will be signed and maintained by the following individuals:

Non-criminal Agency Coordinator (NAC): The agency head of each non-criminal justice agency will designate a NAC to act as the primary contact person for that agency (Appendix D). The NAC shall complete LSP Bureau training requirements and shall serve as the point of contact and 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.

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, including agency, contractor, and/or vendor personnel. 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 the LSP Bureau.

Local Agency Security Officer (LASO): Pursuant to the CJIS Security Policy, the non-criminal justice agency is required to appoint 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 have knowledge of IT security procedures (Appendix B). LASOs are designated as the point of contact on security-related issues for their respective agencies and are responsible for instituting the LSP Bureau's incident response reporting procedures at their agency as needed (Appendix C). It is the LASO's responsibility to ensure the day to day security of the CHRI and ensure the agency's CHRI policies and procedures are enforced, maintain information security documentation, assist the NAC with audits, and keep LSP informed as to any information security needs and problems. It is not uncommon for the NAC and LASO to be the same person within an agency. See the section titled "Incident Response" for more information related to the duties of the LASO.

I have read and acknowledged the above information. _____

Initials

Security Awareness Training and Authorized Personnel

Only authorized personnel within a non-criminal justice agency can view, access, or interact with the criminal history record information (CHRI). To be considered authorized personnel, the individuals that require access to the CHRI must complete CJIS Security Awareness Training.

The LSP Bureau provides CJIS Security Awareness Training to all non-criminal justice agencies. This training is completed through an online training and certification resource known as CJIS Online, and includes a course and certification. The NAC for each agency will be given an account by the LSP Bureau and it is the NAC's responsibility to manage users and ensure the training is complete and current for all individuals at their agency who require access to CHRI. The NAC is responsible for ensuring agency personnel with access to CHRI receive this training within six (6) months of employment, job assignment, or access to CHRI, and recertify every year thereafter.

For the NAC to access the Security Awareness Training, follow the below link and credentials.

Link to the training: cjisonline.com
Username: NAC email address provided to the LSP Bureau on the User Agreement
Password: The NAC will be required to change the password upon the initial login

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 I).

The requirement for Security Awareness Training is found in the CJIS Security Policy, Section 5.2 Awareness and Training (AT).

I have read and acknowledged the above information. _____

Initials

Applicant Notification and Record Challenge

Applicant Rights and Privacy Statements

The National Crime Prevention and Privacy 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 Non-criminal Justice Applicant's document (Appendix E). A non-criminal justice agency must notify applicants of their privacy rights by providing applicants with a copy of the Non-criminal Justice Applicant's Privacy Rights document (Appendix F) prior to sending an applicant to be fingerprinted. Information is also available in the Privacy Act Statement (Appendix G) and accessible through the link below.

Privacy Act Statement: https://www.fbi.gov/services/cjis/compact-council/privacy-act-statement

Non-criminal Justice Applicant's Privacy Rights:
https://www.fbi.gov/services/cjis/compact-council/guiding-principles-noncriminal-justice-applicants-privacy-rights

State and Federal Record Challenge

If a NCJA receives CHRI results that contain disqualifying charges without a final court disposition, or that the applicant determines are inaccurate, the NCJA must provide a reasonable time for the applicant to correct or complete their record. Currently, neither the FBI nor the LSP Bureau have defined what qualifies as a "reasonable time", therefore it is the responsibility of the NCJA to determine a reasonable time for this process and ensure it is documented in their agency policies. If an applicant elects to correct or complete their record, the NCJA cannot make an eligibility determination until the conclusion of the reasonable time.

NCJAs are required to advise the applicant of the procedures for obtaining changes, corrections, or updates to their criminal record. Information on the processes for challenging a state and federal record are below.

Right to Review - State Record Challenge

Pursuant to LA Revised Statute 15:588, an individual can obtain a certified copy of their personal criminal history record as maintained by the LSP Bureau. Individuals must submit a Right to Review Authorization Form (Appendix M) and a Right to Review Disclosure Form (Appendix N) along with fingerprints and the appropriate fees to the LSP Bureau. 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, an authorized representative, or an attorney.

State website for information about record review and challenge:

https://lsp.org/about/leadershipsections/support/bcii/fingerprints-and-background-checks/

FBI Identity History Summary checks - Federal Record Challenge

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 and forms:

https://www.fbi.gov/services/cjis/identity-history-summary-checks

I have read and acknowledged the above information. _____

Initials

Security of Criminal History Record Information (CHRI)

Non-criminal justice agencies (NCJA) must have written policies and procedures regarding and specific to the access, use, dissemination, and disposal of CHRI. These policies and procedures must be made available to LSP Bureau personnel or the Louisiana CJIS Information Security Officer (ISO) upon request. The following subsections outline the required policies that must be in place along with guidance on protecting the security and confidentiality of the CHRI. **Sample policies are found in Appendix J**.

Acceptable Use Policy

A non-criminal justice agency (NCJA) shall have a written policy identifying the use of CHRI and stating that the records shall only be used for official purposes and will not be disseminated outside of the agency to unauthorized entities. This policy should also reference the specific reason the agency is requesting CHRI (for example, for the purpose of employment or licensing) and include the agency's statutory authority or applicant type. The statutory authority and applicant type will be provided by the LSP Bureau prior to the non-criminal justice agency receiving CHRI.

The requirement for an acceptable use policy is found in Public Law 92-544 and Title 28, C.F.R. 20.33, and 50.12(b).

Storage of Criminal History Record Information (CHRI) Policies

Non-criminal justice agencies (NCJA) have the option to store CHRI either physically, in hard copies, or electronically, on a computer or in an electronic system. The LSP Bureau recommends storing CHRI physically to ease the burden of the non-criminal justice agency in protecting the security and confidentiality of the records. When a NCJA stores the CHRI physically, a physical protection policy is required. When a NCJA stores the CHRI electronically, both a physical protection policy and a media protection policy are required. Details of each policy are described in the subsections below.

CHRI includes the actual results received from fingerprint-based background checks along with any documentation identifying the existence or non-existence of CHRI. Maintaining an external tracking system identifying such an existence is considered to be CHRI and will need to meet the appropriate storage requirements.

Physical Protection Policy

Agencies are required to establish appropriate administrative 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, and specific to CHRI, 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. An example of this type of secure storage would be maintaining the CHRI records in a locked file cabinet, in a locked room, only accessible to authorized personnel.

Controlled Areas

If an agency cannot meet all of the controls required for establishing a physically secure location (description available in CJISSECPOL v.5.9.5, Section 5.9 Physical and Environmental Protection (PE), PE-17 Alternate Work Site), but has an operational need to access or store CHRI, the non-criminal justice agency shall designate an area, a room, or a storage container, as a controlled area for the purpose of day-to-day CHRI access or storage. To be considered a controlled area, the NCJA shall:

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

A NCJA must specify in their CHRI physical protection policy that the records are stored in a controlled area.

Physical Security includes:

- Protection of the criminal history record information as confidential.
- Limitation of visitor access to controlled areas.
- Positioning of computer and system devices (laptops, cellular phones, I-pads, or any kind of handheld devices used to access, process, or store CHRI media) in such a way that prevents unauthorized personnel from 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 if the personnel file could be accessible to individuals who are unauthorized to view or access the CHRI.

The requirements for a physical protection policy are found in the CJIS Security Policy, Section 5.9.

Media Protection Policy

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. The NCJA must have procedures written, and specific to CHRI, in their agency policy for securely handling, transporting, and storing electronic CHRI.

Electronic Security includes:

- Restricting access to the digital/electronic CHRI and the systems/computers the records are on to authorized individuals.
- Password use and management.
- Protection from viruses, worms, Trojan horses, and other malicious code.
- Appropriate use and management of e-mail, spam, and attachments.
- 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).

The requirements for a media protection policy and electronic storage/access to CHRI are found in the CJIS Security Policy, listed in this document as Appendix A.

Criminal History Record Information (CHRI) Retention Policy

A non-criminal justice agency (NCJA) may store criminal history record information in hard copy (physical) format or electronic format. The CHRI 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. **A NCJA must have a written policy stating the duration of time the CHRI is maintained within the agency.** If a retention timeframe is mandated per the NCJA's statutory authority to receive CHRI, or by a governing entity's record retention guidelines, this would also need to be stated in the agency's policy with the specific timeframe.

Criminal History Record Information (CHRI) Destruction Policies

At the end of the NCJA's retention timeframe, CHRI shall be destroyed. There are specific requirements for the destruction of CHRI that must be followed and included in the NCJA's CHRI destruction policy. **When a NCJA stores the CHRI physically, the agency is required to have a Physical Destruction Policy. When a NCJA stores the CHRI electronically or digitally, the agency is required to have a Media Sanitation and Disposal Policy.**

Physical Destruction Policy

To compliantly destroy physical CHRI, a NCJA has two options. The NCJA must choose one of these options to destroy the CHRI and ensure it is properly documented in the agency's policies.

Option 1: Physical CHRI will be shredded by cross shredding and witnessed or performed by authorized personnel within the agency.

Option 2: Physical CHRI will be incinerated and witnessed or performed by authorized personnel within the agency.

Media Sanitation and Disposal Policy

To compliantly destroy and sanitize electronic CHRI, a NCJA has three options. The NCJA must choose one of these options to destroy the electronic CHRI and ensure it is properly documented in the agency's policies.

Option 1: The NCJA will sanitize the electronic CHRI by overwriting the data at least three times prior to disposing of or reusing the computer/device/system the electronic CHRI was stored on. Overwriting the CHRI data must be completed or witnessed by authorized personnel within the agency.

Option 2: The NCJA will degauss the electronic CHRI prior to disposing of or reusing the computer/device/system the electronic CHRI was stored on. Degaussing the CHRI data must be completed or witnessed by authorized personnel within the agency. (Degaussing is neutralizing a magnetic field to erase information from a magnetic disk or other storage device).

Option 3: If the computer/device that the CHRI data is stored on is no longer operational, the NCJA must physically destroy the device. Destruction of the device containing electronic CHRI must be completed or witnessed by authorized personnel within the agency.

Disciplinary and Misuse of Criminal History Record Information (CHRI) Policy

A non-criminal justice agency (NCJA) must have a written policy outlining the steps they will take if it is identified that there has been a misuse of CHRI. This policy must minimally include the following:

- Using CHRI for any purpose other than what is allowed by state statute or Federal code is considered misuse.
- The specific steps your agency will take in the event intentional misuse is discovered.
- Misuse of CHRI can result in loss of access to CHRI, loss of employment, and/or criminal prosecution.
- Misuse of CHRI shall be reported to the state.

The requirements for a Disciplinary Policy are found in the CJIS Security Policy, Section 5.12.4 Personnel Sanctions.

Incident Response Policy

The non-criminal justice agency's (NCJA) LASO is responsible for all security-related issues and instituting the LSP Bureau's incident response reporting procedures at their agency, as needed. **To fulfill this responsibility, the NCJA must have a written Incident Response Policy.**

The CHRI Incident Response Policy must:

- 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, including the LSP CJIS ISO.

The requirements for an Incident Response Policy are found in the CJIS Security Policy, Section 5.3 Incident Response.

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 H).

I have read and acknowledged the above information. _____

Initials

Outsourcing

If a non-criminal justice agency (NCJA) shares or disseminates the criminal history record information (CHRI) the agency receives with a third party entity (e.g. separate department, governmental agency, non-governmental entity, county IT, or vendor/service provider) for any purpose, including but not limited to storage, disposal, or eligibility determinations, the NCJA must first complete the Outsourcing Approval Process. A NCJA cannot distribute CHRI to a third party or store the CHRI in a software solution without first obtaining approval from the LSP Bureau.

When a NCJA elects to outsource, the NCJA is taking on additional responsibilities to ensure the security and confidentiality of the CHRI they are authorized to receive.

To ensure that the state and federal requirements for secure handling, storage, and destruction of CHRI are being met, the Outsourcing Approval Process exists to vet third parties and/or software solutions that are being provided access to CHRI by the NCJA. The approval process includes an audit of the third party/software solution and a review of the contract or agreement with the NCJA authorized to receive the CHRI.

When a NCJA elects to outsource, the agency is taking on additional responsibilities to ensure the security and confidentiality of the CHRI they are authorized to receive.

To begin the Outsourcing Approval Process, a NCJA must email *LSP.BCII.NCJA@la.gov* with the subject line "Starting the Outsourcing Approval Process". The following must be included in the body of the email request:

- Name of the third party or software the NCJA is seeking to share the CHRI with or store the CHRI in.
- The purpose for the dissemination (storage, disposal, eligibility determinations, etc.)
- The name, phone, and email for the point of contact within the contractor.

If a NCJA is unsure if they need outsourcing approval, reach out to *LSP.BCII.NCJA@la.gov* for assistance.

I have read and acknowledged the above information. _____

Initials

Audit

Non-criminal Justice Agencies (NCJA) that are authorized to receive CHRI for non-criminal justice purposes are subject to an audit to ensure compliance with state and federal rules regarding fingerprint submissions and CHRI use. The NCJA will be audited once in every three year audit cycle in order to assess compliance with state and federal policies and regulations. The NCJA may also be audited by the FBI during the FBI audit of the Louisiana State Police.

The LSP Bureau's Non-Criminal Justice Agency Audit Program is conducted through an online system called CJIS Audit. The NCJA will be notified of their login credentials and access to the audit 30 days prior to audit assignment. The audit questionnaire will assess a NCJA's level of compliance with the state and federal requirements around accessing, storing, and maintaining CHRI as described, but not limited to the information, in this packet. Below is a timeline of the audit process:

- ☐ 30 days prior to the NCJA audit being issued, the LSP Bureau or representatives will email the NCJA to validate contact information
- ☐ Once contact information is confirmed, a pre-audit questionnaire will be issued
- ☐ The NCJA must complete and submit the pre-audit questionnaire within 15 days
- ☐ 30 days after the initial audit notification email is sent, the NCJA Audit will be issued
- ☐ The NCJA must complete and submit the NCJA Audit questionnaire within 15 days
- ☐ The LSP Bureau or representatives will review the audit and develop a report including the initially identified areas of non-compliance
- ☐ The NCJA must respond to each item on the report with further information, corrective action plans, and/or estimated dates of correction within 15 days
- ☐ The LSP Bureau or representatives will conduct a final review of the audit and monitor non-compliant findings through correction

I have read and acknowledged the above information. _____

Initials

Appendices

Appendix A	**FBI CJIS Security Policy**
Appendix B	**Local Agency Security Officer (LASO) form**
Appendix C	**Security Incident Reporting form**
Appendix D	**Non-criminal Agency Coordinator (NAC) form**
Appendix E	**Agency Privacy Requirements for Non-criminal Justice Applicants**
Appendix F	**Non-criminal Justice Applicant's Privacy Rights**
Appendix G	**Privacy Act Statement**
Appendix H	**OTS Information Security Policy**
Appendix I	**Statement of Misuse**
Appendix J	**Sample Policies**
Appendix K	**Background Check Authorization Form**
Appendix L	**LAPS Authorization Form**
Appendix M	**Right to Review Authorization Form**
Appendix N	**Right to Review Disclosure Form**

Acknowledgement of Requirements

Please email a signed copy of this entire document to LSP.BCII.NCJA@la.gov and keep a copy for your records.

_____	_____	_____
Signature of Agency Head	Title and Printed Name	Date
_____	_____	_____
Signature of Agency NAC	Title and Printed Name	Date
_____	_____	_____
Signature of Agency LASO	Title and Printed Name	Date