Outsourcing Information 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
ARSO	Authorized Recipient 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

Definitions

Authorized Recipient (AR): A noncriminal justice agency (NCJA) that has been approved by the FBI to submit fingerprints and receive and review CHRI as part of a volunteer, employment, or licensing approval process; or a government agency authorized by federal statute, federal executive order, or state statute approved by the U.S. Attorney General to receive CHRI for noncriminal justice purposes. According to federal law, only the AR can have access to the CHRI that has been requested for this process. For consistency in terminology, the AR will be referred to as the NCJA throughout this document except in a direct reference to the requirements found in the Outsourcing Standard for Non-Channelers.

Authorized Recipient Security Officer (ARSO): The individual appointed by the Authorized Recipient (AR) to coordinate and oversee Information Security by ensuring that the Contractor is adhering to the CJISSECPOL and Outsourcing Standard, verifying the completion of annual Awareness and Training Program, and communicating with the FBI CJIS Division on matters relating to Information Security. The ARSO must be an employee of the AR, and the ARSO role cannot be outsourced.

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).

Contractor: The entity, organization, or person who supports the Authorized Recipient (AR) in this process which requires access to CHRI. A government agency, a private business, non-profit organization or individual, that is not itself an Authorized Recipient (AR) with respect to the particular noncriminal justice purpose, who has entered into an outsourcing agreement with an AR to perform noncriminal justice administrative functions requiring access to CHRI. The term Contractor also includes a subcontractor(s) that has contracted with a Contractor and supports the outsourced noncriminal justice administrative functions being performed by the Contractor on behalf of the AR.

CVVP: The Centralized Vendor Vetting Process is a Louisiana State Police (LSP) program implemented to provide state level CJIS screening for vendors working with criminal justice agencies in Louisiana. This program is managed by LSP's Technology and Business Support unit, the LSP CJIS Team (LCJIS), and the Office of Technology Services.

Dissemination: The disclosure of CHRI by an Authorized Recipient (AR) to an authorized Contractor, or by the Contractor to another AR consistent with the Contractor's responsibilities and with limitations imposed by federal and state laws, regulations, and standards as well as rules, procedures, and standards established by the Compact Council and the U.S. Attorney General.

Outsourcing: The process in which any entity, organization, or person, other than the Non-Criminal Justice Agency, provides noncriminal justice administrative or information technology support to the NCJA as part of the CHRI review process. Essentially outsourcing is when someone (or entity) else supports or helps the NCJA complete their assigned task/function with the CHRI. Any work related to request, suitability determination, storage and disposal of CHRI that is performed by another government agency or contractor is considered outsourcing. A NCJA MUST obtain approval from LSP prior to contracting or engaging in outsourcing.

Outsourcing Agreement: A contractual agreement between an Authorized Recipient (AR) and a Contractor, in which the Contractor agrees to perform noncriminal justice administrative functions requiring access to

CHRI on behalf of the AR. When outsourcing occurs between governmental agencies, the outsourcing agreement may be an interagency agreement.

Outsourcing Standard for Non-Channelers: A document approved by the Compact Council after consultation with the U.S. Attorney General which establishes rules and guidelines for an Authorized Recipient and a Contractor. Pursuant to 28 CFR part 906, this Outsourcing Standard authorizes access to CHRI for noncriminal justice purposes, limits the use of the information to the purposes for which it is provided, prohibits retention and/or dissemination except as specifically authorized, ensures the security and confidentiality of the information, provides for audits and sanctions, provides conditions for termination of the outsourcing agreement, and contains such other provisions as the Compact Council may require.

Introduction

A non-criminal justice agency (NCJA) must complete the Outsourcing Approval Process when they elect to share or disseminate the criminal history record information (CHRI) the agency receives with a third party entity (e.g. separate department, governmental agency, parish IT, or vendor/service provider) for any purpose, including but not limited to storage, disposal, or eligibility determinations. An NCJA cannot distribute CHRI to a third party without first obtaining approval from the State Compact Officer.

When an 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 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.

This packet will provide the information and instructions NCJAs need in order to obtain outsourcing approval.

Access to Criminal History Record Information (CHRI)

A non-criminal justice agency (NCJA) can only receive criminal history record information (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 only receive state results. An NCJA cannot receive the results of background checks without a statutory authority.

Overview of Outsourcing Approval Process Steps

This section will provide a roadmap of the steps required to obtain outsourcing approval. Details for each step are provided in the following sections. If at any time in the Outsourcing Approval Process the non-criminal justice agency (NCJA) decides not to continue with the outsourcing request, the NCJA must email LSP.BCII.NCJA@la.gov informing the Louisiana State Police (LSP) of their withdrawal.

1. The NCJA emails *LSP.BCII.NCJA@la.gov* requesting to outsource.
2. The LSP provides the NCJA the Outsourcing Information Packet and Outsourcing Request Form.
3. The NCJA submits the signed Outsourcing Information Packet and the completed Outsourcing Request Form to the LSP.
4. The LSP will review the NCJA's statutory authority, and if approved, the LSP will send the NCJA a blank Outsourcing Agreement.
5. The NCJA executes and submits the Outsourcing Agreement to the LSP.
6. The LSP will assign the NCJA and the Contractor an Outsourcing Audit.
7. The NCJA and the Contractor must complete the audit and submit required documentation.
8. The NCJA and the Contractor must respond and correct non-compliant findings from the audit.
9. The NCJA must ensure the Contractor personnel complete fingerprint based background checks (if the NCJA conducts fingerprint based background checks of their employees).
10. The LSP will make an approval determination for the outsourcing request.

11. (If Approved) The LSP will provide the NCJA with instructions on how to maintain the outsourcing approval.

Request to Outsource

This packet has been sent to the Non-Criminal Justice Agency (NCJA) due to a request to begin the Outsourcing Approval Process. In order to complete the request, this packet must be returned to *LSP.BCII.NCJA@la.gov* along with the completed Outsourcing Request Form.

Outsourcing Request Form

The Request Form must be completed and returned to *LSP.BCII.NCJA@la.gov* within 15 days from receiving the Outsourcing Packet from the Louisiana State Police (LSP). If upon reading through the outsourcing requirements the NCJA determines they will withdraw their outsourcing request, the NCJA will contact LSP through the above email informing them of the cancellation.

Outsourcing Agreement

The Compact Council's Outsourcing Standard for Non-Channelers requires a written document that binds both parties, via signature, to the requirements of the Outsourcing Standard and the CJIS Security Policy. The NCJA and the Contractor must execute the Outsourcing Agreement provided via email. This agreement requires authorized signatures from the contractor and the NCJA, and identifies the CJIS-related services being performed (outsourcing). The Outsourcing Agreement must be submitted with the signed Outsourcing Information Packet and Outsourcing Request Form to complete the Outsourcing Approval Request.

I have read and acknowledged the above information. _____

Initials

Training and Background Checks

The contractor employees with access to CHRI are required to complete CJIS Security Awareness Training. This training is completed through CJIS Online and includes a course and certification. The Non-Criminal Justice Agency (NCJA) will inform the Contractor of the training requirement and create the Contractor's CJIS Online account if one does not already exist.

If the Contractor's personnel have already completed CJIS Security Awareness Training through CJIS Online, the NCJA's Authorized Recipient Security Officer (ARSO) must ensure the training certificates are up to date. The NCJA's ARSO is responsible for ensuring Contractor personnel with access to CHRI receive this training within six (6) months of employment, job assignment, or access to CHRI, and annually thereafter.

All Contractor 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 B).

Background Checking Contractor Employees

If the NCJA requesting outsourcing approval conducts fingerprint-based background checks on their employees, then the Contractor employees must receive a fingerprint-based background check. The NCJA must have the statutory authority for these employee background checks. The statute does not need to specifically state that the background check is done *for access to CHRI,* however, the statute could state that all employees at the NCJA must/can have a fingerprint-based background check completed.

If the NCJA and Contractor qualify for these fingerprint-based background checks, LSP will inform the contractor of the fingerprint submission instructions after the completion of the Outsourcing Audit, prior to granting outsourcing approval.

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 specific to the access, use, dissemination, and disposal of CHRI. When an NCJA elects to outsource, the Contractor is also responsible for these same policy requirements. Additionally, the NCJA must incorporate the Contractor in their agency's CHRI policies as defined below. The following subsections outline the required policies that must be in place for the Contractor along with guidance on protecting the security and confidentiality of the CHRI. Details on the required policies for the NCJAs can be found in the Louisiana Non-Criminal Justice Agency Onboarding Packet.

These policies and procedures must be made available to LSP personnel or the Louisiana CJIS Information Security Officer (ISO) upon request.

Storage of Criminal History Record Information (CHRI) Policies

When a Contractor performing outsourced non-criminal justice agency functions stores the CHRI physically, a physical protection policy is required. When a Contractor 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 CHRI and will need to meet the appropriate storage requirements.

Physical Protection Policy

Contractors performing outsourced non-criminal justice agency functions 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. Contractors must have these procedures written, and specific to CHRI, included in their policy. This includes maintaining the CHRI in a secure location that is not readily accessible to individuals not authorized to see it.

Controlled Areas

If a Contractor cannot meet all of the controls required for establishing a physically secure location, but has an operational need to access or store CHRI, the Contractor 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 Contractor 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 Contractor must specify in their CHRI physical protection policy that the records are stored in a controlled area.

Physical Security includes:

- Protection of the CHRI as confidential.
- Limitation of visitor access to controlled areas.
- Positioning of computer and system devices (laptops, cellular phones, ipads, or any kind of handheld 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.

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 Contractor must have procedures written and specific to CHRI in their 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)

Criminal History Record Information (CHRI) Retention Policy

A Contractor must have a written policy stating the duration of time the CHRI is maintained. A Contractor cannot retain CHRI longer than the NCJA's retention policy. Additionally, the Contractor cannot retain the CHRI after the Outsourcing Agreement between the NCJA and the Contractor ends. If the Outsourcing Agreement ends prior to the retention schedule, the Contractor must dispose of the CHRI immediately upon the completion/termination of the Outsourcing Agreement.

Criminal History Record Information (CHRI) Destruction Policies

At the end of NCJA's retention timeframe or the completion/termination of the Outsourcing Agreement, the Contractor's CHRI shall be destroyed. There are specific requirements for the destruction of CHRI that must be followed and included in the Contractor's CHRI destruction policy. **When a Contractor stores the CHRI physically, the agency is required to have a Physical Destruction Policy. When a Contractor 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 Contractor has two options. The Contractor must choose one of these options to destroy the CHRI and ensure it is properly documented in the Contractor's policies.

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

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

Media Sanitation and Disposal Policy

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

Option 1: The Contractor 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.

Option 2: The Contractor 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. (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 Contractor must physically destroy the device. Destruction of the device containing electronic CHRI must be completed or witnessed by authorized personnel.

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

A Contractor 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 the Contractor 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.

Additionally, the NCJA must include the Contractor employees in the NCJA's CHRI Misuse Policy.

Incident Response Policy

The Contractor is responsible for all security-related issues involving CHRI. **To fulfill this responsibility, the Contractor 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.

In the event of an incident involving CHRI, the Contractor must notify the NCJA within one (1) hour of discovery. The Contractor must provide the NCJA with a written report documenting the security violation, the corrective actions taken by the Contractor to resolve the violation, and the date, time, and summary of the violation within five (5) calendar days.

Additionally, the NCJA must include the Contractor employees in the NCJA's CHRI Incident Response Policy.

In the event of a security incident with the Contractor involving CHRI, the NCJA must notify the LSP State Compact Officer at LSP.BCII.NCJA@la.gov within one (1) hour of receiving the notification from the Contractor. The NCJA must provide the LSP State Compact Officer with a written report documenting the security violation, the corrective actions taken by the NCJA, and the applicable Contractor's name; a summary of the violation, the date and time of the violation, whether the violation was intentional, and the number of times the violation occurred. This report must be provided to the LSP State Compact Officer within five (5) calendar days.

SOC II/Type II Attestation

To assess the contractor's overall organizational security posture including corporate networks, policies, and any developed applications, each contractor shall be required to submit a SOC II/Type 2 attestation. If the

contractor has not completed a SOC II/Type 2 attestation, a full Vendor Vetting IT Audit Questionnaire shall be assigned to the contractor at the time of the Outsourcing audit.

I have read and acknowledged the above information. _____

Initials

Outsourcing Audit

The Outsourcing Audit is conducted through an online system called CJIS Audit. The Outsourcing Audit is designed to be answered by the NCJA with cooperation from the Contractor. As the majority of the responsibility around enforcing the Outsourcing Standards falls on the NCJA, it is crucial that they are aware of the contractor's answers to the audit questions and compliance level. The NCJA and Contractor points of contact will be given login credentials to the CJIS Audit system.

The Outsourcing Audit includes questions related to Personnel Security, CHRI Dissemination, Security of CHRI, Technical Security of CHRI, and Incident Reporting. The audit questions, in their entirety, are provided to the NCJA and the Contractor at the end of this document. These are provided to ensure the NCJA and the Contractor have appropriate time to prepare for the audit.

Audit Timeline

- ☐ Once the Outsourcing Request is confirmed, LSP will assign the Outsourcing Audit.
- ☐ The NCJA and the Contractor must complete and submit the audit **within 30 days**.
- ☐ LSP will conduct the initial review of the audit and develop a compliance report of the identified areas of non-compliance.
- ☐ The NCJA and the Contractor must respond to each item on the compliance report with further information, corrective action plans, and/or estimated dates of correction **within 30 days.**
- ☐ The LSP OTS will conduct a final review of the audit and monitor non-compliant findings through correction.

Required Artifacts

The following artifacts are required to be submitted for review as part of the audit process. If these are not in place and compliant, the outsourcing request will be denied.

NCJA:

- ☐ Disciplinary Policy
- ☐ Incident Response Policy

Contractor:

- ☐ Disciplinary Policy
- ☐ Physical/Media Protection Policy
- ☐ Retention Policy

- ☐ CHRI Destruction Policy
- ☐ SOC II/Type II Attestation
- ☐ Network Diagram

I have read and acknowledged the above information. _____

Initials

Subcontractor to the Contractor

The Outsourcing Standard for Non-Channelers, Section 3.14, states that the Contractor **shall not disseminate CHRI** without the consent of the NCJA. As such, the Louisiana State Police will not allow approved contractors to utilize subcontractors for the outsourcing of non-criminal justice functions.

I have read and acknowledged the above information. _____

Initials

Outsourcing Approval & Denial

Upon completion of the Outsourcing Audit, the Louisiana State Police (LSP) Compact Officer will make an approval decision. If the instance of outsourcing is approved, the LSP will email the Non-Criminal Justice Agency (NCJA) an Outsourcing Approval letter and a Post-Approval Maintenance Instructions document. If the instance of outsourcing is denied, the LSP will provide the NCJA an Outsourcing Denial Letter.

I have read and acknowledged the above information. _____

Initials

Post-Approval Maintenance

Now that you have received outsourcing approval, here are some things to keep in mind.

- The State Compact Officer may suspend your agency's access to CHRI or suspend/terminate the exchange of CHRI with your Contractor for:
    - a PII breach or security violation,
    - the failure to notify the State Compact Officer of a PII breach or security violation, or
    - the refusal/incapability to take corrective action to successfully resolve a PII breach or security violation. (28 CFR section 906.2(d))
        - The State Compact Officer may reinstate your agency's access to CHRI or the exchange of CHRI between your agency and the Contractor after receiving written assurance(s) of corrective action(s) from your agency and/or the Contractor.
- The State Compact Officer reserves the right to investigate or decline to investigate any report of unauthorized access to CHRI.

- The State Compact Officer is authorized to perform a final audit of the Contractor's system following termination of an outsourcing agreement.
- Your agency may initiate a termination of its outsourcing agreement with the Contractor due to the following:
    - The Contractor commits a PII breach or security violation involving access to CHRI obtained pursuant to the outsourcing agreement.
    - The Contractor fails to notify your agency of a PII breach or security violation or to provide a written report of a violation.
    - The Contractor refuses to, or is incapable of, taking corrective actions to successfully resolve a PII breach or security violation.

The Outsourcing Standard for Non-Channelers provides specific timeframes for notification of incidents or contract termination after outsourcing has been approved. A breakdown of these timeframes is listed below, categorized by responsibility.

Non-Criminal Justice Agency (NCJA) Responsibility:

- ☐ The NCJA shall ensure the most updated version of the Outsourcing Standard and the CJISSECPOL are incorporated by reference at the time of outsourcing agreement, outsourcing agreement renewal, or within the 60-day notification period of updates to the Outsourcing Standard and the CJISSECPOL, whichever is sooner.
- ☐ The NCJA shall notify the State Compact Officer and the FBI of any PII breach or security violation within one hour of notice from the Contractor.
    - ☐ The NCJA shall also provide a written report of any PII breach or security violation (to include unauthorized access to CHRI by the Contractor) to the State Compact Officer within five calendar days of receipt of the initial notification from the Contractor.
    - ☐ The written report must include corrective actions taken by the NCJA and, if necessary, the Contractor to resolve the issue; the applicable Contractor's name; a summary of the violation; the date and time of the violation; whether the violation was intentional; and the number of times the violation occurred.
- ☐ The NCJA shall provide written notice of any early voluntary termination of the outsourcing agreement with the Contractor to the Compact Officer/Chief Administrator.
- ☐ The NCJA shall make its facilities available for announced and unannounced audits and security inspections performed by the state or the FBI on behalf of the Compact Council.

Contractor Responsibility:

- ☐ The Contractor shall maintain updated records of employees who have access to CHRI, update those records within 24 hours when changes to employee access occurs, and if a criminal history record check is required, maintain a list of personnel who have successfully completed criminal history record checks.

- ☐ The Contractor shall notify the NCJA via an agreed upon method within one-business day when additions or deletions occur to authorized personnel.

☐ The Contractor shall immediately (within one hour) notify the NCJA of any criminal history record information (CHRI) breach.

☐ The Contractor must provide the NCJA with a written report documenting security violation, corrective actions taken by the Contractor to resolve the violation, and the date, time, and summary of the violation within five (5) calendar days.

☐ The Contractor shall make its facilities available for announced and unannounced audits and security inspections performed by the NCJA, the state, or the FBI on behalf of the Compact Council.

☐ The Contractor must also permit the NCJA, the state, or the FBI to review its network configuration as it relates to the outsourced function(s) upon request.

I have read and acknowledged the above information. _____

Initials

Appendices

Appendix A FBI CJIS Security Policy
https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center

Appendix B Statement of Misuse
https://lsp.org/media/2umcenr2/statement_of_misuse.pdf

Appendix C 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

Appendix D Outsourcing Agreement
https://lsp.org/media/gghlsbxr/outsourcing-agreement.pdf

Appendix E Contractor Employee Outsourcing Acknowledgement Form
https://lsp.org/media/k02emeca/contractor-employee-outsourcing-acknowledgement-form.pdf

Appendix F Security Incident Reporting Form
https://lsp.org/media/cp0guv4m/outsourcing-security-incident-reporting-form-1.pdf

Appendix G Outsourcing Request Form
https://lsp.org/media/nlslzfn0/outsourcing-request-form.pdf

Audit Questions

Introduction

1. For the purposes of this audit the following definitions apply:

   Non-Criminal Justice Agency (NCJA): The authorized recipient (AR) of criminal history record information (CHRI) with the statutory authority to receive the CHRI for noncriminal justice purposes (e.g., employment, volunteers, licensing, etc.).

   Contractor: A third-party that an NCJA is sharing their CHRI with under contract for services that include, but are not limited to, eligibility determinations, storage and disposal of CHRI, and IT functions.

2. This audit will assess the responsibilities of both the NCJA and the Contractor for the Outsourcing Approval Process. The NCJA must work with the Contractor to answer the questions in this audit.

   Each question will identify who is responsible (the NCJA or the Contractor) for the requirement being assessed.

3. Briefly describe the reason the NCJA has an agreement with the Contractor that allows access to CHRI and is requesting Outsourcing Approval (e.g. storage, disposal, eligibility determinations, etc.).

Personnel Security

4. Question for the NCJA:

   Does your agency have an Authorized Recipient Security Officer (ARSO)?

   a. Question for the NCJA:

      When a NCJA elects to Outsource, the ARSO is additionally responsible for the below tasks.

      - Documenting the NCJA's technical compliance with this Outsourcing Standard

      - Establishing a security incident response and reporting procedure to discover, investigate, document, and report on major incidents that significantly endanger the security or integrity of the noncriminal justice agency systems to the CJIS Systems Officer, SCO/Chief Administrator and the FBI CJIS Division Information Security Officer.

      Is your agency ARSO familiar with these additional responsibilities?

5. Question for the Contractor:

   Have all of the contractor employees that have access to CHRI, through the contract with the NCJA, completed CJIS Security Awareness Training in CJIS Online?

6. Question for the Contractor:

   Have all of the employees that have access to CHRI, through the agreement with the NCJA, signed the Contractor Employee Outsourcing Acknowledgement Form?

   b. Question for the Contractor:

      Are all employee signed certifications filed and retained for review?

   c. Question for the Contractor:

      The Contractor is required to ensure that each employee has certified in writing that he/she understands the Outsourcing Standard requirements and laws that apply to his/her responsibilities. The Contractor shall maintain the employee certifications in a file that is subject to review during audits. Employees shall make such certification prior to performing work under the outsourcing agreement.

      Please download a copy of the Contractor Employee Outsourcing Acknowledgement Form to distribute to each employee and maintain for future audits.

7. Question for the Contractor:

   Does the contractor ensure the CHRI is only accessible to authorized personnel who completed the CJIS Security Awareness Training?

8. Question for the NCJA:

   Does your agency maintain a list of the contractor employees authorized for access to CHRI through the Outsourcing Agreement?

   d. Question for the Contractor:

      Does your organization notify the NCJA of changes to the authorized personnel list within 24 hours of the change?

9. Question for the Contractor:

   Does the contractor have a written policy defining actions taken when an employee commits a violation of the security provisions of your contract with the Authorized Recipient?

   e. Please upload a copy of the Contractor's Disciplinary/Personnel Sanctions Policy as a PDF for review.

10. Question for the NCJA:

Does your agency have a written policy for the discipline of Contractor employees who violate the security provisions of the Outsourcing Agreement?

f. Please upload a copy of the NCJA's Disciplinary/Personnel Sanctions Policy as a PDF for review.

CHRI Dissemination

11. Question for the NCJA:

    Describe how your agency provides the contractor with the CHRI records?

    (e.g. upload into the contractor's software, handling physical/paper copies of the CHRI, secure digital transmission)

12. Question for the Contractor:

    Do you maintain a dissemination log of the sharing of/providing access to CHRI with the NCJA?

    g. Question for the Contractor:

       Describe the fields that are included in the dissemination log.

    h. Question for the Contractor:

       Are the dissemination logs maintained for at least one year?

13. Question for the Contractor:

    Does the contractor disseminate the CHRI or provide access to another entity that is not the NCJA where the records originated?

Security of CHRI

14. Question for the Contractor:

    Does the contractor have a written policy that specifies the procedures for the handling, transporting and storing of physical (i.e. printed) or electronic media containing CHRI by authorized persons?

    i. Question for the Contractor:

       Is CHRI stored in a physically secure location (e.g., locked room, locked file cabinet) where access is permitted for ONLY the contractor employees that have been approved for access to CHRI?

    j. Question for the Contractor:

       Please upload a copy of the Contractor's Physical/Media Protection Policy as a PDF for review.

15. Question for the NCJA:

Has the NCJA informed the contractor of the agency's CHRI retention timeframe?

16. Question for the Contractor:

    Does the contractor maintain the CHRI records longer than the NCJA's retention timeframe?

17. Question for the Contractor:

    Does the contractor have documented procedures regarding how long the CHRI you receive from the NCJA will be stored?

    k. Question for the Contractor:

       Does the contractor retain CHRI after the agreement with the NCJA is completed/terminated?

    l. Question for the Contractor:

       Please upload a copy of the Contractor's CHRI Retention Policy as a PDF for review.

18. Question for the Contractor:

    Does the contractor have documented procedures for how the CHRI will be destroyed, either as part of the contracted service or after the retention period?

    m. Question for the Contractor:

       Please upload a copy of the Contractor's CHRI Destruction Policy as a PDF for review.

19. Question for the Contractor:

    When destroying physical (paper) CHRI, does the contractor ensure the records are cross-shredded or incinerated by authorized personnel?

20. Question for the Contractor:

    When destroying electronic CHRI, what method of sanitation does the contractor use?

Technical Security of CHRI

21. The following section asks questions regarding components of the Contractor's Security Program, in compliance with the CJIS Security Policy and the Outsourcing Standard for Non-Channelers. Each of the topics discussed in this section should be documented by the contractor in their internal CHRI Security Program.

22. Question for the Contractor:

    Does your company have a SOC 2 / Type II attestation?

n. Question for the Contractor:

Please upload a copy of the Contractor's SOC 2 / Type II Attestation as a PDF for review.

o. Question for the Contractor:

The Contractor will receive an additional IT Security Audit Questionnaire to assess the technical solution with access to CHRI. This audit will not be completed until the IT Audit Questionnaire is returned.

23. Question for the Contractor:

The storage and/or transmission of digital CHRI requires additional policies and protections to ensure CHRI is only accessed by authorized persons. The following questions will assess key components of your technology security.

As it relates to digital/electronic CHRI, if you do not transmit, receive, access or store digital CHRI you should reply N/A to the following questions.

24. Question for the Contractor:

Does your agency employ boundary protection devices (e.g. proxies, gateways, firewalls, routers, encrypted tunnels) to ensure criminal history record information and services are secured against unauthorized access and use?

Note - this includes ensuring agency email and/or web servers are firewalled, on a separate DMZ and are not accessible to the internet).

25. Question for the Contractor:

Is CHRI transmitted outside of a physically secure location?

Examples of "transmitted" include, but are not limited to, emailing, viewing information stored in the cloud, on line or on a server; copying and pasting to a server located in another building, copying into an application on the internet.

p. Question for the Contractor:

Is electronically transmitted CHRI (i.e. CHRI in transit) encrypted by a FIPS 140-3 certified cryptographic module?

q. Question for the Contractor:

Please upload a copy of the Contractor's NIST certificate as a PDF for review.

NIST certificates can be obtained at the following NIST website: https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search

26. Question for the Contractor:

    Has the Contractor implemented signature-based malicious code protection software to detect and eradicate malicious code in your network?

27. Question for the Contractor:

    Are all company personnel with access to the digital/electronic criminal history record information (CHRI) uniquely identified (i.e. there are no generic usernames or accounts)?

28. Question for the Contractor:

    Is access to the location where the digital/electronically stored criminal history record information (CHRI) protected by a password or some other form of authentication?

    r. Question for the Contractor:

    Does your organization:

    1. Maintain a list of commonly-used, expected, or compromised passwords via API or download from a third party. Update the list quarterly and when organizational passwords are suspected to have been compromised directly or indirectly. Compare current passwords against the list quarterly;

    2. Require immediate selection of a new password upon account recovery;

    3. Allow user selection of long passwords and passphrases, including spaces and all printable characters;

    4. Employ automated tools to assist the user in selecting strong password authenticators;

    5. If chosen by the subscriber, passwords SHALL be at least 8 characters in length.

    6. If chosen by the CSP or verifier using an approved random number generator, passwords SHALL be at least 6 characters in length.

    7. Truncation of the password SHALL NOT be performed.

    8. Password verifiers SHALL NOT permit the subscriber to store a "hint" that is accessible to an unauthenticated claimant.

    9. Verifiers SHALL NOT prompt subscribers to use specific types of information (e.g., "What was the name of your first pet?") when choosing passwords.

    10. When processing requests to establish and change passwords, verifiers SHALL compare the prospective secrets against the list maintained as required by IA-5(1)(a)(1) that contains values known to be commonly used, expected, or compromised.

11. If a chosen password is found in the list, the CSP or verifier SHALL advise the subscriber that they need to select a different password.

12. If a chosen password is found in the list, the CSP or verifier SHALL provide the reason for rejection.

13. If a chosen password is found in the list, the CSP or verifier SHALL require the subscriber to choose a different value.

14. Verifiers SHALL implement a rate-limiting mechanism that effectively limits failed authentication attempts that can be made on the subscriber's account to no more than five.

15. Verifiers SHALL force a change of password if there is evidence of compromise of the authenticator.

16. The verifier SHALL use approved encryption when requesting passwords in order to provide resistance to eavesdropping and MitM attacks.

17. The verifier SHALL use an authenticated protected channel when requesting passwords in order to provide resistance to eavesdropping and MitM attacks.

18. Verifiers SHALL store passwords in a form that is resistant to offline attacks.

19. Passwords SHALL be salted and hashed using a suitable one-way key derivation function.

20. The salt SHALL be at least 32 bits in length and be chosen arbitrarily to minimize salt value collisions among stored hashes.

21. Both the salt value and the resulting hash SHALL be stored for each subscriber using a password authenticator.

22. If an additional iteration of a key derivation function using a salt value known only to the verifier is performed, then this password salt value SHALL be generated with an approved random bit generator and of sufficient length.

23. If an additional iteration of a key derivation function using a salt value known only to the verifier is performed, then this password salt value SHALL provide at least the minimum-security strength.

24. If an additional iteration of a key derivation function using a salt value known only to the verifier is performed, then this password salt value SHALL be stored separately from the passwords.

29. Question for the Contractor:

Any information system that stores CHRI must be capable of logging; successful and unsuccessful log-on attempts, user account/file/directory permission changes (i.e. create, write, delete, change),

password changes, audit log activities including access, modification or deletion and actions by privileged accounts (i.e. root, Oracle, DBA, Admin, etc)

Is your company's information system where criminal history record information (CHRI) is stored capable of generating audit records for the above defined events that are relevant to the security of the system (e.g. login attempts, password changes, privilege changes)?

s. Question for the Contractor:

Are audit records periodically reviewed for unusual activity and maintained for a minimum of one year?

30. Question for the Contractor:

Does the contractor maintain a network diagram depicting the interconnectivity of the network as it relates to electronic CHRI?

t. Question for the Contractor:

Please upload a copy of the Contractor's Network Diagram as a PDF for review.

The submitted diagram should include the following:

1. All communications paths, circuits, and other components used for the interconnection of the network as it relates to electronic CHRI indicating the vendor system and end-point(s). The diagram should not include network addresses.

2. 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.

3. 'For Official Use Only' (FOUO) markings.

4. The vendor name and date (day, month, and year) drawing was created or updated.

Incident Reporting

31. Question for the Contractor:

Do you have a written Incident Response Policy for use when there are suspected or proven incidents of misuse of CHRI or unauthorized access to CHRI?

u. Question for the Contractor:

Please upload a copy of the Contractor's Incident Response Policy as a PDF for review.

32. Question for the NCJA:

Has the NCJA's CHRI Incident Response Policy been updated to include the Contractor Personnel?

v. Question for the NCJA:

Please upload a copy of the NCJA's Incident Response Policy as a PDF for review.

33. Question for the Contractor:

When suspected incidents of misuse or unauthorized access of CHRI are identified, do you notify the State Compact Officer within 1 hour?

w. Question for the Contractor:

Within 5 days of the reported incident, do you provide a written report to the NCJA, documenting the date/time of the security incident, a summary of the incident, and corrective actions taken?