## Table of Contents

| | | | |
|---|---|---|---|
| **Procedure #:** | 22.01.000 | **Effective Date:** | April 1, 2018 |
| **Supersedes:** | NCJA Manual 2013 Edition | **See Also:** | |
| **Applies To:** | All NCJA Users | **CALEA:** | |

## I. INTRODUCTION AND BACKGROUND

A. The Washington State Patrol (WSP) is required by the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division, to audit noncriminal justice agencies that conduct fingerprint based background checks within the state of Washington for noncriminal justice purposes such as licensing, child placement, and/or HUD housing determinations

## II. ROLES AND RESPONSIBILITIES

A. A noncriminal justice agency (NCJA) designated to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions, shall be eligible for access to criminal justice information (CJI). Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. An NCJA receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority of the CJIS Systems Agency (CSA) providing the access.

B. The FBI CJIS Division establishes rules to maintain system integrity, which all user agencies must abide by. These rules are defined in the CJIS Security Policy.

1. The CJIS Security Policy provides Criminal Justice Agencies (CJA) and NCJAs with a minimum set of security requirements for access to Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division systems and information and to protect and safeguard CJI. These minimum standards of security requirements ensures continuity of information protection. The essential premise of the CJIS Security Policy is to provide the appropriate controls to protect CJI, from creation through dissemination; whether at rest or in transit.

2. The CJIS Security Policy integrates presidential directives, federal laws, FBI directives, the criminal justice community's Advisory Policy Board (APB) decisions along with nationally recognized guidance from the National Institute of Standards and Technology (NIST) and the National Crime Prevention and Privacy Compact Council (Compact Council).

C. Each CSA that accesses NCIC shall be audited at least once every three years by the FBI CJIS audit staff. This audit shall include a sample of state and local noncriminal justice agencies. The objective of this audit is to verify adherence to FBI CJIS policy and regulations and is termed a compliance audit.

D. The WSP is designated by the FBI as the CSA. The CSA is a criminal justice agency which has overall responsibility for the administration and usage of the FBI's CJIS Division programs within their jurisdiction. The WSP is the manager of the 'state switch' known as A Central Computerized Enforcement Service System (ACCESS). The CSA is also responsible for establishing and administering an information technology security program. The CSA may impose more stringent protection measures than defined by the NCIC Operating Manual and CJIS Security Policy.

E. The head of each CSA shall appoint a CJIS Systems Officer (CSO). The CSO is an individual located within the CSA responsible for the administration of the CJIS network for the CSA. The CSO for Washington State is the WSP Criminal Records Division Administrator. The ACCESS Section is designated to train, audit and provide assistance to all NCJAs within the state.

F. The Terminal Agency Coordinator (TAC) serves as the point-of-contact at the local agency for matters relating to CJIS information access. The TAC administers CJIS systems programs within the local agency and oversees the agency's compliance with ACCESS and CJIS systems policies.

G. An Information Technology (IT) point of contact must be designated at each noncriminal justice agency. The technical point of contact administers CJIS systems programs within the local agency and oversees the agency's compliance specifically related to the technical requirements with ACCESS and CJIS systems policies.

## III. USE OF CHRI AND DISSEMINATION

A. Criminal History Record Information (CHRI) cannot be shared with any internal or external body not involved in the fitness determination of an applicant, outlined in the authorized recipient's statutory authority. CHRI may be given to the applicant upon written request and requires the applicant's identity be verified. The delivery of CHRI to the applicant can be mailed via USPS mail, after a waiver has been signed by the applicant requesting a copy. When CHRI is given to an applicant, it should be logged by the NCJA and retained for one year.

B. The authority for an NCJA to disseminate or share CHRI with another NCJA must be approved by the CSA. The request to disseminate CHRI must be concurrent with the Compact Council, *Outsourcing Standard* established by the Privacy Compact Council and the CJIS Security Policy. A written agreement must be accomplished between the authorized recipient of CHRI and the other NCJA with whom the authorized recipient is requesting to share CHRI.

## IV. USE OF CHRI STORAGE AND RETENTION

A. Hard copy CHRI records shall be stored in a physically secure environment as defined in the CJIS Security Policy.

B. Agencies are encouraged to NOT store electronic CHRI in any format as a best practice to ensure data protection. However, if electronic CHRI records are stored, they must be protected following all minimum requirements detailed in the CJIS Security policy, including FIPS 140-2 Certified encryption of at least 128bit strength, audit logging, and restricted account access.

C. When CHRI is stored, agencies shall establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of the information. CHRI records shall only be kept as long as absolutely necessary for the purpose of which they were obtained and shall be destroyed as soon as possible.

## V. FINGERPRINT PROCESS

A. Fingerprints, with the Originating Agency Identifier (ORI) and reason added, shall be submitted to the Washington State Patrol (WSP) for processing and forwarding to the Federal Bureau of Investigation (FBI).

B. Each NCJA is required to have a written fingerprint process procedure that will be reviewed during audits. A template is available on the ACCESS webpage for use if acceptable documentation does not exist.

C. It is the responsibility of the agency collecting the fingerprints to inform the person being fingerprinted of the authority to collect the information and its potential use. Civil fingerprint submissions are often collected manually on FBI applicant cards (FD-258) or via electronic fingerprint capturing devices (such as livescan). This information is then provided to authorized agencies in support of federal criminal history checks. Those persons being fingerprinted on the FD-258 fingerprint cards are required to provide a signature for verification and authorization purposes at the time of fingerprinting. If an agency uses a livescan device to capture fingerprints for noncriminal justice purposes, the CJIS Division staff recommends that the agency implement an electronic signature capability to provide a copy of the back of the FD-258 for the applicant to sign, indicating that the applicant understands the potential use of submitted fingerprints.

D. In addition, officials making the determination of suitability for licensing and employment purposes “shall provide the applicant the opportunity to complete, or challenge the accuracy of the information contained in the FBI identification record.” These officials must also advise the applicant of the procedures for obtaining a change, correction, or update to an FBI identification record as set forth in Title 28, Code of Federal Regulations (CFR) Section 16.34. A statement incorporating the use and challenge requirements is required to be placed on records disseminated for these purposes.

| | | | |
|---|---|---|---|
| **Procedure #:** | 22.02.000 | **Effective Date:** | April 1, 2018 |
| **Supersedes:** | NCJA Manual 2013 Edition | **See Also:** | |
| **Applies To:** | All NCJA Users | **CALEA:** | |

## I. AUTHORTIES

A. The noncriminal justice use of CHRI audit is based on the following guidelines, where applicable.

1. Title 5, United States Code (U.S.C.), Section 552, the Freedom of Information Act, requires the records be accurate, complete, timely, and relevant.
2. Title 5, U.S.C., Section 552a, the Privacy Act, requires that agencies maintain a system of records which establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records.
3. Title 28, U.S.C., Section 534, authorizes dissemination of CHRI, and provides that access to CHRI is subject to cancellation if dissemination is made outside of the authorized recipient.
4. Title 28, Code of Federal Regulations (CFR), 20.30, cites the administration of criminal justice shall include criminal identification activities, and the collection, storage and dissemination of CHRI.
5. Title 28, CFR, 20.33 (a) (2), authorizes the dissemination of CHRI contained in the III to federal agencies authorized to receive it pursuant to federal statute or Executive Order.
6. Title 28, CFR, 20.33 (a) (3), authorizes the dissemination of CHRI contained in the III for use in connection with licensing or employment, pursuant to Public Law (Pub. L.) 92-544, 86 Stat. 1115, or other federal legislation, and for other uses for which dissemination is authorized by federal law.
7. Title 28, CFR, 50.12 (b), references the exchange of FBI identification records obtained under this authority may be used solely for the purpose requested and cannot be disseminated outside the receiving departments, related agencies, or other authorized entities.
8. Title 28, CFR, Part 906, Outsourcing of Noncriminal Justice Administrative Functions, amends the dissemination restrictions of 28 CFR 50.12 (b), by permitting the outsourcing of noncriminal justice history record checks to either another governmental agency

or a private contractor acting as an agent for the authorized receiving agency. Published as a final rule on December 15, 2005, this rule also established the standards, entitled the Security and Management Control Outsourcing Standard (Outsourcing Standard) that must be followed for an agency to outsource these functions.

9. Title 28, CFR, Part 906, the Outsourcing Standard, requires contractors to maintain a security program consistent with federal and state laws, regulations, and standards, as well as, with rules, procedures, and standards established by the Compact Council and the United States Attorney General. The Outsourcing Standard identifies the duties and responsibilities with respect to adequate internal controls within the contractual relationship so that the security and integrity of the III System and criminal history information are not compromised. The security program shall include consideration of site security, dissemination restrictions, personnel security, system security, and data security.

10. Title 42, U.S.C., Chapter 140, Subchapter II, Section 14616, the National Crime Prevention and Privacy Compact (Compact), established the Compact Council, which is authorized to establish rules, procedures, and standards for the use of Interstate Identification Index (III) for noncriminal justice purposes. Determining compliance includes, but is not limited to: assessing participation requirements; the continual maintenance; and security of CHRI.Public law (pub.l) 92-544

    a. The FBI is empowered to exchange identification records with officials of state and local governments for purposes of licensing and employment; authorized by a state statute which has been approved by Washington State legislature.

11. Public Law 101-630: Federal law titled *Indian Child Protection and Family Violence Prevention* that requires Tribes to check criminal backgrounds for anyone working, volunteering, or having regular contact or control over Indian children, including foster home placements (checking the people the child is going to be living with). This will only ever be used with Tribal agencies.

12. Public Law 105-276(sec 578)/104-120(sec 9b)/42 U.S.C. 1437d (q)(1)): Housing and Urban Development act that allows housing authorities to check for criminal records.

| | |
|---|---|
| **CHAPTER 22:** | **NCJA** |
| **SECTION 03:** | **ESTABLISHING A NONCRIMINAL JUSTICE AGENCY (NCJA)** |

| | | | |
|---|---|---|---|
| **Procedure #:** | 22.03.000 | **Effective Date:** | April 1, 2018 |
| **Supersedes:** | NCJA Manual 2013 Edition | **See Also:** | |
| **Applies To:** | All NCJA Users | **CALEA:** | |

## I. ESTABLISHING A NONCRIMINAL JUSTICE AGENCY (NCJA) - NEW LEGISLATION

A. Workflow process

1. The requesting agency drafts legislation.
2. WSP reviews the legislation and forwards it to the FBI for review to ensure it meets the criteria of Public Law 92-544 which authorizes the FBI to release criminal history information for noncriminal justice employment purposes.
3. The FBI will either approve or provide recommended changes.
4. The requesting agency will make recommended changes if necessary, prior to submitting to the legislature.
5. The agency will submit the draft legislation to the legislature for passing.
6. Once passed, WSP and the requesting agency will work together in establishing a process. Normally by the agency submitting a letter to WSP with the intention of enacting the legislation.
7. The WSP will send a letter to the FBI requesting final approval of the passed legislation.
8. The FBI approves and assigns and ORI number and reason fingerprinted.
9. The WSP sends the requesting agency a confirmation letter of the ORI number assignment.
10. WSP adds the ORI and the reason fingerprinted to the FBI response table, database ORI table and WASIS.
11. An ACCCESS Section business auditor contacts the NCJA to perform a new agency review and site security visit.
    a. As part of this process, required policies and procedures are reviewed and confirmed to be applicable to the NCJA
12. The requesting agency will set up a billing account with WSP for submitting state/federal fingerprint searches.

B. Example of wording for draft legislation

1. *The investigation shall consist of a background check as allowed through the Washington state criminal records privacy act under RCW 10.97.050, the Washington state patrol criminal identification system under RCW 43.43.832 through 43.43.834, and the Federal Bureau of Investigation (FBI). These background checks will be done through the Washington state patrol criminal identification section and may include a national check from the FBI, which shall be through the submission of fingerprints.*

## II. NONCRIMINAL JUSTICE AGENCY (NCJA) – CHANGES TO EXISTING LEGISLATION

A. Workflow process

1. The requesting agency drafts legislation with changes pertaining to the fingerprint based background checks.
2. The WSP reviews and forwards to the FBI for review to ensure it meets criteria of Public Law 92-544 which authorizes the FBI to release criminal history information for noncriminal justice employment purposes.
3. The FBI will either approve or provide recommended changes.
4. The requesting agency will make recommended changes if necessary, prior to submitting to the legislature.
5. The agency will submit the draft legislation to the legislature for passing.
6. Once passed, WSP and the requesting agency will work together in establishing a process. Normally by the agency submitting a letter to WSP with the intention of enacting the legislation.
7. The WSP will send a letter to the FBI requesting final approval of the passed legislation.
8. The FBI approves the legislation.
9. The WSP sends the requesting agency a confirmation letter of approval.

## III. ORI ISSUANCE – NAMING CONVENTION

A. **Z-ORI:** NCJA ORI for either PL 92-544 or PL 101-630 based statutes.

B. **Q-ORI:** NCJA ORI for Housing Authorities based on PL 105-276/104-120/42 U.S.C. 1437d(q)(1)). In certain cases, they may receive name/DOB III checks from a PD (usually Tribal).

C. **T-ORI:** NCJA ORI for emergency placement of children, based on PL 92-544 and RCW 26.44.240.

1. Name/Date of Birth III Check (QWH/QR) is submitted by the PD/DCYF at the time of emergency placement using the T-ORI. Within 15 days, the child welfare agency must submit fingerprints on the same person using the T-ORI.

   Because this is affecting both a criminal justice agency and the noncriminal justice agency the T-ORI is assigned to, two audits are

required. The CJA audit asks questions about the T-ORI, but a separate NCJA audit is need to check compliance for the CHRI responses from the fingerprint submissions.

| | | | |
|---|---|---|---|
| **Procedure #:** | 22.04.000 | **Effective Date:** | April 1, 2018 |
| **Supersedes:** | NCJA Manual 2013 Edition | **See Also:** | |
| **Applies To:** | All NCJA Users | **CALEA:** | |

## I. SYSTEM RESPONSIBILITY

A. The WSP, as the state CSA, is responsible for system security and its enforcement for all other agencies it services.

B. The WSP and the FBI use hardware and software controls to help ensure system security. However, final responsibility for the maintenance of the security and confidentiality of CHRI rests with the individual agencies. Further information regarding system security can be obtained from the FBI's CJIS Security Policy.

## II. TARGET AREAS FOR SECURITY

A. System Security

1. ACCESS strictly adheres to the CJIS Security Policy. The policy can be found at https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center

2. All agencies must have a physically secure location as defined by the CJIS Security Policy:

   a. A physically secure location is a facility, a criminal justice conveyance, or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CHRI and associated information systems. The perimeter of the physically secure location shall be prominently posted and separated from non-secure locations by physical controls. Security perimeters shall be defined, controlled, and secured.

3. Every physical access point to sensitive facilities or restricted areas housing information systems that access, process, or display CHRI data shall be controlled/secured in a manner which is acceptable to the CSO during both working and non-working hours.

B. Destruction

1. Destruction of CHRI shall be conducted only by NCJA employees who have taken CJIS Security Awareness training (Level 2 or 4) in the past two years.

2. Physical media shall be securely disposed of when no longer required, using formal procedures. Formal procedures for the

secure disposal or destruction of physical media shall minimize the risk of sensitive information compromise by unauthorized individuals. Physical media shall be destroyed by cross-cut shredding or incineration.

3. Electronic media when it has reached end of life or is no longer going to be used, that has ever been used to store or process CHRI, shall be sanitized (overwritten three times), Degaussed, or physically destroyed to prevent unintended release of CHRI data. Inoperable electronic media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. This includes photocopier hard drives.

## III. ENCRYPTION STANDARDS

A. Any CHRI data 'in motion', must be encrypted using Federal Information Processing Standard (FIPS) 140-2 certified algorithms and use a symmetric cipher key strength of at least 128 bit strength, as required by the CJIS Security Policy.

B. Any CHRI data 'at rest' must be encrypted using FIPS 140-2 certified algorithms and use a symmetric cipher key strength of at least 128 bit strength, or AES256.

C. Agencies are strongly encouraged to NOT save or transfer CHRI data once it is received from WSP in PDF format.

## IV. FIREWALLS

A. Agencies must adhere to the CJIS Security Policy with regard to the required firewalls.

## V. IDENTIFICATION AND AUTHENTICATION

A. Each individual's identifier/password shall be authenticated at either the local interface agency or CSA level.

## VI. NETWORK DIAGRAM

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

## VII. SECURITY INCIDENTS OF CHRI DATA

### A. Incident Response

1. The security risk of both accidental and malicious attacks against government and private agencies, remains persistent in both physical and logical environments. To ensure protection of Criminal Justice Information (CJI), agencies shall:

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

B. **Reporting Security Events**

1. Agencies shall promptly report incident information to the ACCESS Information Security Officer (ISO) by email to ACCESS@wsp.wa.gov using the *FBI Security Incident Reporting Form* available on the ACCESS webpage: http://www.wsp.wa.gov/_secured/access/docs/cjis_security_incident_report_form.pdf to any authorities appropriate to the local agency.

2. Security events, including identified weaknesses associated with the event, shall be communicated in a manner allowing timely corrective action to be taken. Formal event reporting and escalation procedures shall be in place. Wherever feasible, the agency shall employ automated mechanisms to assist in the reporting of security incidents. All employees, contractors and third party users shall be made aware of the procedures for reporting the different types of events and weakness that might have an impact on the security of agency assets and are required to report any security events and weaknesses as quickly as possible to the designated point of contact.

C. **Management of Security Incidents**

1. A consistent and effective approach shall be applied to the management of security incidents. Responsibilities and procedures shall be in place to handle security events and weaknesses effectively once they have been reported.

D. **Incident Handling**

1. The agency shall implement an incident handling capability for security incidents that includes; preparation, detection and analysis, containment, eradication, and recovery. Wherever feasible, the agency shall employ automated mechanisms to support the incident handling process.

2. Incident-related information can be obtained from a variety of sources including, but not limited to; audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. The agency should incorporate the lessons learned from ongoing incident handling activities into the incident response procedures and implement the procedures accordingly.

E. **Collection of Evidence**

1. Where a follow-up action against a person or agency after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

| | | | |
|---|---|---|---|
| **Procedure #:** | 22.05.000 | **Effective Date:** | April 1, 2018 |
| **Supersedes:** | NCJA Manual 2013 Edition | **See Also:** | |
| **Applies To:** | All NCJA Users | **CALEA:** | |

## I. REGULATIONS

A. Title 28, U.S.C., § 534, Pub. L. 92-544, Pub. L 101-630 and Title 28, CFR, 20.33(b), provide that the exchange of records and information is subject to CANCELLATION if dissemination is made outside the receiving departments or related agencies. 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. Penalties may be different depending on the authority to which the CHRI was authorized for dissemination.

B. If an agency suspects an employee of obtaining information from any Washington State Patrol (WSP) supported system, including from fingerprint submission or from the Washington Access to Criminal History (WATCH or WATCH-CJ) online system for unauthorized purposes, the WSP ACCESS Section must be notified.

## II. REPORTING

A. The ACCESS Section will provide the agency with an NCJA Violation Incident Report to complete and return. The agency must investigate the alleged misuse and provide all data requested to ACCESS via the Incident Report. The report can be found at;

http://www.wsp.wa.gov/_secured/access/docs/noncriminal_justice_violation_report.pdf

B. If the misuse is confirmed, the agency may choose their own disciplinary actions (training, time off, termination, etc.). A report of the disciplinary action must be provided to the ACCESS Section.

C. When employee misuse is founded, additional sanctions may be imposed by the ACCESS Section. The manager of the ACCESS Section, in consultation with the WSP Criminal Records Division Administrator, will determine if a misuse warrants further sanctions, up to disallowing further use of the WSP supported services.

| | | | |
|---|---|---|---|
| **Procedure #:** | 22.06.000 | **Effective Date:** | April 1, 2018 |
| **Supersedes:** | NCJA Manual 2013 Edition | **See Also:** | |
| **Applies To:** | All NCJA Users | **CALEA:** | |

## I. NCJA TERMINAL AGENCY COORDINATOR (TAC)

A. All Noncriminal Justice Agencies (NCJA) that receive CHRI from fingerprint submissions must designate a point of contact within their agency who will serve as a liaison for matters relating to CHRI information. This person is referred to as the TAC.

## II. NCJA TAC REQUIREMENTS

A. Must maintain an agency issued email address.

B. A Memo 550 must be completed whenever there is a TAC, agency head, or technical point of contact change; address change; telephone number change; etc.

## III. NCJA TAC RESPONSIBILITIES

A. The TAC acts as the point of contact for CHRI matters.

B. The TAC must be available for the NCJA audits.

1. ACCESS Auditors will contact the TAC during the triennial audit process.

C. The TAC is required to be aware of the required contracts and agreements with WSP, FBI and other entities, if applicable.

D. The TAC must advise the ACCESS Section immediately of any alleged CHRI misuse. For more information, refer to the Misuse Section of this chapter.

E. The TAC must maintain current records of Security Awareness Training for all personnel who have access to CHRI.

F. The TAC must review and update required written procedures.

G. The TAC must respond to requests for information by the FBI NCIC or ACCESS in the form of questionnaires, surveys, or other methods.

| | | | |
|---|---|---|---|
| **Procedure #:** | 22.07.000 | **Effective Date:** | April 1, 2018 |
| **Supersedes:** | NCJA Manual 2013 Edition | **See Also:** | |
| **Applies To:** | All NCJA Users | **CALEA:** | |

## I. SECURITY AWARENESS TRAINING

A. Basic security awareness training shall be required within six months of initial assignment, and biennially thereafter, for all personnel who have unescorted access to unencrypted CHRI.

B. Security awareness training is the responsibility of the agency. All NCJAs will be responsible for:

1. Keeping a current list of authorized employees who are allowed access to CHRI.
2. Be able to show that the employee received the awareness training.

C. Security awareness training is to be completed using CJIS online.

| | | | |
|---|---|---|---|
| **Procedure #:** | 22.08.000 | **Effective Date:** | April 1, 2018 |
| **Supersedes:** | NCJA Manual 2013 Edition | **See Also:** | |
| **Applies To:** | All NCJA Users | **CALEA:** | |

## I. AUDIT STANDARDS

A. The NCJA business audit and NCJA technical security audit both conform to FBI and state standards.

B. The ACCESS audit team shall conduct both compliance audits triennially of each NCJA with the ability to receive CHRI in order to verify compliance with applicable statutes, regulations and policies. Compliance audits may be conducted on a more frequent basis if the audit reveals that an agency has not met the compliance standards.

C. The audit cycle will be concurrent with the Criminal Justice Agency audit cycle.

D. The purpose of the audit is to assess compliance with noncriminal justice use and the appropriate rules pertaining to the security, maintenance, and dissemination of CHRI.

E. Audits focus on two areas:

1. Agency compliance
2. Recommendations to lessen agency liability

F. The triennial audit calendar is located on the ACCESS webpage. The audit schedule is subject to change without advance notice.

http://www.wsp.wa.gov/_secured/access/training.htm

## II. NCJA BUSINESS AUDIT

A. ACCESS Audit Process

1. Approximately two months prior to the NCJA audit, the ACCESS Auditors send notification of the upcoming audit to the TAC and agency head.
2. Approximately one month prior to the NCJA audit, the ACCESS Auditors will ask the agency to provide their statutory authority, submit procedures, outsourcing agreements if applicable and logs of all personnel who have reviewed the security awareness training within CJIS online.

3. Approximately one week prior to the NCJA audit, the auditor will contact the TAC to advise of the time of the audit and which files will be reviewed.

4. The NCJA audit is conducted with the TAC for each agency.

    a. If a TAC has not been assigned, then the agency head will be contacted to complete the audit.

5. Auditors will review the following, if applicable:

    a. Written Procedures
    b. Outsourcing Agreements
    c. Security Awareness Logs
    d. Files of Fingerprint Submissions

6. Auditors will conduct site security visits to ensure LiveScan locations and areas where CHRI may be stored are secure. The following areas will be reviewed during the site security visits:

    a. Who has access, including unescorted access, to the site
    b. Who performs the cleaning/facilities maintenance at the site
    c. Method of disposal for CHRI media

7. Upon completion of the audit, the auditor will complete an exit interview with the TAC and the agency head, if available. The auditor will provide the final compliance report at this time.

8. The auditor reviews all findings with the agency and provides the TAC their login credentials for CJIS Audit to respond to the compliance report

    a. Have the TAC print off copies of the report for all who will be attending the exit interview
    b. Write the due date on the report, which should be at least 30 days from the date the audit was conducted. Due dates are always the 1st or the 15th, whichever is closest to 30 days post-audit.

        (1) Example: If the audit was conducted on 9/7, then it would be due on 10/15

    c. Agencies must respond to numbered compliance items in writing within 30 days of the final summary report.
    d. If the original 30 days lapses and the agency has not responded to the original report, the auditor will contact the agency to check on the status of the response. The ACCESS Section Manager and/or Information Security Officer (ISO) will be advised.
    e. If the agency still has not responded, the auditors will turn the audit file over to the ACCESS Section Manager and/or the ISO. The Section Manager or ISO will work with the Criminal Records Division (CRD) Administrator to reach the agency and complete the audit process.

f. Follow up audits may be conducted depending on findings. This will be at the discretion of the WSP whether it is a telephone conference or an additional on-site sanction audit.

B. NCJA Audit Non-Compliance

1. Failure to comply with established policies and procedures may be cause for sanctions. Sanctions will be determined by the ACCESS Auditor, ACCESS Section Manager, and the CRD Division Administrator. Possible sanctions may include, but are not limited to:

a. A formal letter to agency head
b. Discontinuance of service

C. Agencies will receive a certificate of completion indicating that the audit has been completed once all compliance issues have been addressed.

D. NCJA Audit Questions

1. For questions or concerns related to the ACCESS audit, contact the ACCESS Auditors at (360) 534-2010.

## III. NCJA TECHNICAL SECURITY AUDIT

A. The NCJA technical security audit is conducted virtually and reviews an electronic questionnaire completed ahead of time by the TAC and Information Technology Point of Contact (IT POC) in CJIS Audit.

B. NCJA Technical Security Audit Process

1. The auditor will send notification of the upcoming audit to the TAC and IT POC with instructions for accessing the audit questionnaire in CJIS Audit and the audit date.

2. The auditor will contact the agency IT POC as reported by each agency for all technical security audit related questions.

a. If an IT POC has not been assigned, then the TAC will complete the audit.

3. The auditor will review the following, if applicable:

a. Personnel security
b. Security incidents
c. Configuration management
d. Media protection
e. Physical protection
f. Session lock
g. System and communications protection and information integrity
h. Boundary protection
i. Malicious code
j. Event logging
k. System use notification
l. Patch management
m. Identification and authentication
n. Cloud computing

4. Upon completion of the audit, the auditor will provide the agency with a final compliance report and recommendations.

5. The auditor provides a date the agency must respond regarding any needed changes.

    a. Agencies must respond to the compliance items within 30 days of the final summary report.
    b. If the original 30 days lapses and the agency has not responded to the original report, the auditor will call the agency to check on the status of the response.
    c. If the agency still has not responded, the auditor will turn the audit file over to the ACCESS Section Manager. The Section Manager will work with the CRD Administrator to reach the agency and complete the audit process.
    d. Follow up audits may be conducted depending on findings.

C. NCJA Technical Security Audit Non-Compliance

1. Failure to comply with established policies and procedures may be cause for sanctions. Sanctions will be determined by the ISO, ACCESS Section Manager, and the CRD Division Administrator. Possible sanctions may include, but are not limited to:

    a. A formal letter to agency head
    b. Discontinuance of service

2. Agencies will receive a certificate indicating that the audit has been completed once all compliance issues have been addressed.

3. NCJA Technical Security Audit Questions

    a. For questions or concerns related to the NCJA Technical Security Audit, contact ACCESS at (360) 534-2010 or ACCESS@wsp.wa.gov

| | | | |
|---|---|---|---|
| **Procedure #:** | 22.09.000 | **Effective Date:** | May 1, 2012 |
| **Supersedes:** | NCJA Manual 2013 Edition | **See Also:** | |
| **Applies To:** | All NCJA Users | **CALEA:** | |

## I. MEMORANDUM OF UNDERSTANDING (MOU)

A. The MOU sets forth the conditions governing an NCJA's access to CHRI as an authorized recipient either as a nongovernmental entity authorized by federal statute or executive order or as a government agency authorized by federal statute, executive order or state statute by the United States (US) Attorney General to receive CHRI for noncriminal justice purposes. The MOU must be in place between the WSP and the NCJA.

## II. OUTSOURCING

A. Outsourcing of any noncriminal justice agency functions involved with an authorized recipient's authority to receive CHRI is **not authorized**, unless approved by the CSO.

B. A copy of the written approval letter from the CSO must be on file with the agency.

C. If outsourcing is approved by the CSO, the agency's outsourcing agreement must use the approved form and include:

1. Attachment A - SECURITY and MANAGEMENT CONTROL OUTSOURCING STANDARD for NON-CHANNELERS

| | | | |
|---|---|---|---|
| **Procedure #:** | 22.10.000 | **Effective Date:** | May 1, 2012 |
| **Supersedes:** | NCJA Manual 2013 Edition | **See Also:** | |
| **Applies To:** | All NCJA Users | **CALEA:** | |

## I. POLICIES AND PROCEDURES REQUIREMENTS

A. Formal written procedures assist agencies in proper practices and understanding. Agencies must have written procedures on file. The ACCESS Auditors will limit their verification to ensuring the procedures comply with state and federal policy.

B. The ACCESS Section has templates available on the ACCESS webpage for disposal of media, ACCESS misuse, physical protection, outsourcing agreement and a letter requesting outsourcing from the state.

http://www.wsp.wa.gov/_secured/access/forms.htm

1. If used, templates must be modified to reflect agency policies.

C. All written procedures must contain the following:

1. Date the procedures were completed
2. The agency name or letterhead indicated in/on the procedure
3. Details of how a task must be completed

D. ACCESS recommends that all written procedures be reviewed yearly by the agency.

## II. REQUIREMENTS FOR THE NCJA AUDIT

A. ACCESS requires written procedures for the following:

1. NCJA physical protection
2. Destruction of physical media
3. NCJA misuse
4. Fingerprint process

## III. REQUIREMENTS FOR THE NCJA TECHNICAL SECURITY AUDIT

A. ACCESS requires written procedures for the following:

1. Password management
2. Disposal of digital media
3. Data breach reporting