

Show with Compliance Responses

NCJA School Audit Review - T

Section: Introduction

1). Pursuant to state and federal laws, the exchange of criminal history identification records is authorized for the purpose of licensing, employment, or volunteer placement. The most current version of the FBI Criminal Justice Information Services (CJIS) Security Policy provides the minimum standard requirements for the use of Criminal Justice Information (CJI), whether at rest or in transit. These requirements include, but are not limited to: creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI data. This data is commonly referred to throughout the audit review as Criminal History Record Information (CHRI). CHRI access is limited to local, state, and federal governmental agencies authorized to access and receive such CJI data; also known as Noncriminal Justice Agencies (NCJA). All agencies that have access and use CHRI share a responsibility in creating appropriate administrative, technical, and physical safeguards to insure the security, integrity and confidentiality of CHRI.

If your agency has been requested to complete this audit review, it is because you have been determined to be a NCJA receiving fingerprint-based CHRI background checks. Answer the following to the best of your ability. At the end of each section your agency will be provided the opportunity to add additional comments or concerns regarding the audit section.

NCJA means a governmental agency authorized by federal statute, executive order, or state statute and approved by the U.S. Attorney General to be able to receive state and federal fingerprint-based CHRI, directly or indirectly from the Michigan State Police (MSP). Examples of services include, but are not limited to, employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

I have read and understand the above statement.

Section: Supporting Documentation

1). In instances where the agency has requested an individual to complete a fingerprint-based CHRI background check for employment, assignment or to volunteer, is documentation retained that indicates the position offered, assigned to, or volunteered for (e.g. award letter, new hire check list, determination for assignment, volunteer form)?

Note: Position documentation is individualized agency formal documentation in which the position offered or assigned is listed and is a formal document used during the agency hiring or placement process (prior to the fingerprinting of the applicant).

Yes

No

» Primary question answered Yes

1). What type of position documentation is used?

2). Indicate which of the following background check methods the agency uses for any K-12 full time/part time employment with your agency (e.g. professional, administrative, and directly hired staff).

» (Choose All That Apply)

- School Employment (SE)
- NCPA-Child Protection Volunteer (CPV)
- NCPA-Child Protection Employment (CPE)
- Internet Criminal History Access Tool (ICHAT)
- No Background Check Completed

3). Does the agency participate with third party contracting services (e.g. substitute staffing services, janitorial services, Information Technology services, food services, etc.)?

- Yes
- No

1). Provide the business name of the contractor(s), service provided and point of contact: (First/Last Name & Title)

2). Indicate which of the following background check methods the agency uses for individuals assigned to regularly and continuously work under contract (indirectly hired) with your agency (e.g. EduStaff, PESG, Dean, Chartwell's).

» (Choose All That Apply)

- School Employment (SE)
- NCPA-Child Protection Volunteer (CPV)
- NCPA-Child Protection Employment (CPE)
- Internet History Access Tool (ICHAT)
- No background check completed

4). Does the agency participate in Non K-12 Programs (e.g. preschool, daycare, special 4's)?

- Yes
- No

1). Provide program name, type of service and program point of contact: (First/Last Name & Title)

2). Indicate which of the following background check methods the agency uses for the program.

» (Choose All That Apply)

- School Employment (SE)
- NCPA-Child Protection Volunteer (CPV)
- NCPA-Child Protection Employment (CPE)
- Internet Criminal History Access Tool (ICHAT)
- No Background Check Completed

5). Does the agency participate in any additional programs (e.g. camps, MiWorks, AmeriCorps) that require the agency to fingerprint applicants for the program?

Yes

No

1). Provide program name, type of service and program point of contact: (First/Last Name & Title)**2). Indicate which of the following background check methods the agency uses for the program.**

» (Choose All That Apply)

- School Employment (SE)
- NCPA-Child Protection Volunteer (CPV)
- NCPA-Child Protection Employment (CPE)
- Internet Criminal History Access Tool (ICHAT)
- No Background Check Completed

6). Does the agency participate with student teachers?

Yes

No

1). Indicate which of the following background check methods the agency uses for student teachers.

» (Choose All That Apply)

- School Employment (SE)
- NCPA-Child Protection Volunteer (CPV)
- NCPA-Child Protection Employment (CPE)
- Internet Criminal History Access Tool (ICHAT)
- No Background Check Completed

7). Does the agency participate with volunteers (including volunteer coaches)?

Yes

No

1). Indicate which of the following background check methods the agency uses for volunteers.

» (Choose All That Apply)

- School Employment (SE)
- NCPA-Child Protection Volunteer (CPV)
- NCPA-Child Protection Employment (CPE)
- Internet Criminal History Access Tool (ICHAT)
- No Background Check Completed

8). Does the agency obtain applicant's written consent for fingerprinting (Livescan RI-030 form)?

Yes

No

9). Does the agency have a formal appeal process for individuals wishing to challenge, correct, or update their CHRI?

Yes

No

1). Does the agency appeal process include directions for how the applicant may appeal for both an out of state and in state record?

Yes

No

10). Please provide any additional comments regarding the Supporting Documentation audit area. If no further action is needed, please respond with N/A.**Section: User Agreement & Local Agency Security Officer Appointment****1). Does the agency hold an agreement (not Livescan machine agreement) with the Michigan State Police (MSP) granting access for the exchange of CHRI (RI-087-Agency User Agreement for Release of Criminal History Record Information)?**

Yes

No

2). Please indicate your agency's purpose for requesting fingerprint-based background checks in detail and the statutory authority that allows for the fingerprinting.

3). Does the agency have a Local Agency Security Officer (LASO) (An individual, within the agency, that ensures appropriate security measures are in place for CHRI)?

Yes

No

1). Please provide contact information for the LASO. (Name, agency title, email, phone)

Section: Personnel Security

1). Does the agency have an established policy, procedure, written process, or any kind of written documentation that outlines the minimum screening requirements for individuals requiring access to Criminal History Record Information (CHRI)?

Yes

No

2). Does the agency have Contractors and Vendors with access to CHRI?

Note: Contractors and Vendors as used in this area are referring to individuals with Information Technology(IT) type access. This could be a vendor hired for a short time to install or set-up new hardware/ software. While they may not have the direct responsibility of the day to day process of CHRI, the FBI recognizes these individuals as a necessary component to the day to day functionality of the agency. By giving these individuals access to your system and networks, they ultimately have the back door digital (logical access) access to everything (including CHRI).

Yes

No

3). Does the agency have an established policy, procedure, written process, or any kind of written documentation regarding disconnection and/or removal of an employee's access to CHRI responses (physically or digitally) when the employment has been terminated with the agency? (e.g. system access, passwords, building keys, file keys, etc.)

Yes

No

4). Does the agency have an established policy, procedure, written process, or any kind of written documentation regarding the re-evaluation of an employee's CHRI access when reassignment or transfer of agency personnel occurs?

Yes
No

5). Does the agency have formal documentation of sanctions for personnel failing to comply with state or federal laws, current FBI CJIS Security Policy, rules or regulations, including the agency's Information Security Policy?

Yes
No

6). Provide a list of all authorized personnel (can include IT) that have or may have access to CHRI results. (First/Last Name, Directly Hired or Contracted Individuals, Title, and purpose of access)

7). Please provide any additional comments, questions, or concerns regarding the Personnel Security audit area. If no further action is needed, please respond with N/A.

Section: Media Protection

1). Does your agency maintain CHRI digitally (e.g. shared/local drive, cloud services, spreadsheets, system of records)?

Yes
No

1). Explain the agency's handling process for digital CHRI. (Additionally because your agency is storing CHRI digitally you must complete the NCJA Technical Security Questionnaire).

2). Does your agency maintain CHRI by hard copy filing(including manual spreadsheets logging).

Yes

No

3). Does the agency maintain CHRI digitally or physically off-site?

Yes

No

1). Please describe off-site storage details.

4). Does your agency maintain CHRI within a digital system of records? (*If your agency is maintaining CHRI digitally, other than within an email folder, you must complete the Technical Security Questionnaire*).

Yes

No

5). Does the agency have an established policy and procedures in place that addresses the appropriate security controls for the handling, storage, transporting, and destruction of CHRI by an employee of the agency?

Yes

No

6). Explain the agency's "step-by-step" process for the handling of physical CHRI, from the moment it is received, used for the purpose intended, and stored for safe keeping. This process should include where CHRI is physically stored within the agency (HR office, Business office, Personal office, etc.). Also, include any additional or archive areas where CHRI results are physically stored (e.g. use of off-site storage facilities, attic, basement).

7). Does the agency have an established procedure regarding physical destruction of CHRI media?

Yes

No

1). Explain the agency's steps taken for the destruction of physical CHRI media (shredded, burned, kept indefinitely, etc.).

8). Does the agency have established procedures for the appropriate sanitization of digital CHRI media?

Yes

No

1). Explain the agency's steps taken for the destruction of digital CHRI media (references the sanitization or physical destruction of all hard drives, memory devices, mobile devices, or removable transportable digital media used to receive, process, or maintain CHRI).

9). Does the agency have established policy and procedures regarding the agency's transporting of CHRI, whether physical or on digital devices, to places or areas outside of the original place of storage (references how you move CHRI from one place to another, such as storage)?

Yes

No

1). Explain the agency's transport process.

10). Please provide any additional comments, questions or concerns regarding the Media Protection audit area. If no further action is needed, please response with N/A.

Section: Physical Protection

1). NCJAs in receipt of CHRI are required to ensure the security and confidentiality of it. All area(s) where CHRI media is stored and processed are to ensure specific controls are in place for a physically secure location. A physically secure location is a facility, an area, a room, or a group of rooms within a facility. If controls for a physically secure location cannot be met, at a minimum the agency will ensure area(s) where CHRI is processed and maintained meet the requirements for a controlled area. (FBI CJIS Security Policy: Area 5.9) Therefore, this section of the audit will be reviewed on-site by an NCJA auditor for compliance determination.

I have read and understand the above statement.

2). Does the agency ensure that ALL computers and handheld mobile devices used to access CHRI have a firewall in place with current virus, spam and malware protections ?

Yes
No

3). Does the agency allow personally owned devices to access, process CHRI?

Yes
No

1). Does the agency have a documented procedure in place outlining the terms and conditions of use of these devices?

Yes
No

4). Does the agency allow employees to utilize mobile devices (e.g. I-pad, cellular phones) to access CHRI from home or other areas outside of the office?

Yes
No

1). Please indicate device(s) used to access CHRI and by whom.

2). Does agency policy and procedures include agency Mobile Device Management?

Yes
No

3). Does the agency have established additional or enhanced incident reporting and handling procedures to address mobile device operating scenarios?

Yes
No

Section: Incident Response (Digital or Physical CHRI)

1). Does the agency have an established incident response policy and procedure for the reporting of an information security incident involving CHRI media to the appropriate personnel (e.g. LASO, IT personnel, director, agency head, MSP etc.)?

Yes

No

1). Does the agency have an established incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery?

Yes

No

2). Does the agency have established procedures for the collection, retention, and presentation of evidence to the relevant law enforcement jurisdiction(s) for a CHRI security incident involving legal action (either civil or criminal) against a person or agency?

Yes

No

3). Does the agency have established Incident Response Training included as part of the required Security Awareness Training (SAT)?

Yes

No

4). Does the agency have established procedures to track and document information security incidents on an ongoing basis?

Yes

No

2). Please provide any additional comments, questions, or concerns regarding the Incident Response audit area. If no further action is needed, please respond with N/A.

Section: Secondary Dissemination

1). Does the agency share CHRI responses with other agencies or the applicant? (Other than for the purpose of an appeal process.)

Yes

No

1). Is logging or tracking of the secondary dissemination of CHRI completed?

Yes

No

2). In instances where CHRI is shared with another agency, does the agency obtain written consent from the individual allowing the agency prior to releasing the CHRI response?

Yes

No

2). Please provide any additional comments regarding the Secondary Dissemination audit area. If no further action is needed, please respond with N/A.

Section: Security Awareness Training

1). Does the agency conduct Security Awareness Training (SAT) for employees having access to CHRI?

Note: SAT is the basic awareness of the security necessary for authorized personnel having access to CHRI while performing their daily duties. Daily duties may involve the direct/indirect access, or processing of CHRI, and may include IT personnel.

Yes

No

1). Is it the agency's policy to administer and ensure SAT is completed within six months of assignment and every two years thereafter?

Yes

No

2). Is SAT required for all personnel having access to CHRI?

Note: The term "all personnel" includes individuals working on the agency's systems/networks.

Yes

No

2). Please provide any additional comments, questions, or concerns regarding the Security Awareness Training audit area. If no further action is needed, please respond with N/A.

Section: Conclusion

1). In conclusion of the audit questionnaire, we request that you forward any or all of the following documents to the Michigan State Police, Security and Access Section at MSP-CJIC-ATS@michigan.gov. Subject: [Agency Name] Pre-Audit Documents.

1) A copy of your agency's Appeal Process and/or appeal form.

2) A copy of your agency's completed NCJA MSP user agreement (RI-087).

3) Generic example(s) of your agency position documentation(s).

4) A copy of your agency's Livescan (RI-030) form used.

5) Your agency's policy, procedures, or written documentation regarding security, confidentiality, and management controls for CHRI.

6) A copy (generic) of your agency's applicant "consent and release" form used for the release of CHRI to another school for the purpose of employment. (In lieu of a new fingerprint background check being conducted.)

8) If you answered "YES" to question #1 and question #4 (media protection section) about maintaining CHRI digitally you must also complete the NCJA Technical Security Questionnaire.

I have read and will comply.