

## NONCRIMINAL JUSTICE AGENCY USE OF CRIMINAL JUSTICE INFORMATION

PRESENTED BY:  
MICHIGAN STATE POLICE  
CRIMINAL JUSTICE INFORMATION CENTER  
LEIN & CJIS COMPLIANCE SECTION

"A PROUD tradition of SERVICE through EXCELLENCE, INTEGRITY, and  
COURTESY"

1

---

---

---



---

---

---

---

---

## LEIN & CJIS Compliance Section

**Contact Information:**  
LEIN & CJIS Compliance Section  
P.O. Box 30634  
Lansing, Michigan 48909  
517-284-3022 – office  
517-241-0865 – fax

**Website:**  
[www.Michigan.gov/cjicats](http://www.Michigan.gov/cjicats)



**NCJA Email:**  
[MSP-CJIC-ATS@michigan.gov](mailto:MSP-CJIC-ATS@michigan.gov)

**Security & Access Section - Noncriminal Justice Agency (NCJA)**

Welcome to the Michigan State Police (MSP), Security & Access Section (SAS), Noncriminal Justice Agency (NCJA) page. A NCJA is a government agency authorized by federal statute, executive order, or state statute and approved by the U.S. Attorney General to receive state and federal government-based criminal history record information (CHRI), directly or indirectly from the MSP. Purpose is to receive CHRI records that are not related to, employment suitability, licensing information, investigation and reevaluation matters, and national security clearance.

Beginning in 2015, the MSP established a compliance program for agencies requesting CHRI for noncriminal justice purposes. Every agency with noncriminal justice access to state and/or federal criminal history records is required to follow the Federal Bureau of Investigation (FBI), Criminal Justice Information Services (CJIS) Security Policy. The SAS offers training and serves as a resource for these agencies to help ensure compliance with federal and state regulations regarding criminal history records. The SAS personnel also conduct periodic compliance reviews for NCJAs based on the authority of the 28 CFR 161.2. The CJIS 2020 update, CJIS Security Policy and Security and Management Center Outsourcing Standard.

Please take on the right of agency that best describes your services, to find templates, forms, guidance, and audit information.

2

---

---

---



---

---

---

---

---

## Criminal Justice Information

**What is Criminal Justice Information (CJI)?**

- CJI is the term used to describe all the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) provided data, necessary for civil agencies to perform their employment or volunteer placement determinations.

**What is Criminal History Record Information (CHRI)?**

- CHRI is a subset of CJI. Any notations or other written or electronic evidence of an arrest, detention, complaint, information, or other formal criminal charge relating to an identifiable person that includes identifying information regarding the individual, as well as the disposition of any charges.

3

---

---

---


---

---


---

---

---



## Criminal Justice Information Exchange History



**FBI Criminal Justice Information Services**

↓

**Michigan State Police (MSP)**

↓

**Noncriminal Justice Agency (NCJA)**

Serves as the nation's administrator for appropriate security and management controls. As such, the FBI designates one criminal justice agency (on the CJIS network) as the CJIS Systems Agency (CSA) that is considered a point of contact in each state.

The CSA is duly authorized to oversee the security and management of all CJI exchanges within the state of Michigan. Responsible for setting, maintaining, enforcing, and reporting compliance to the FBI CJIS Division for such exchanges.\*\*

For the purpose of licensing and employment, certain authorized agencies request and receive fingerprint-based CHRI, making the NCJAs the next responsible records management entity.

\*\*Title 42 U.S.C., Chapter 140, Subchapter II, 14616; 28 CFR Part 901 § 4, requires MSP SAS to complete NCJA compliance audits.

4

---

---

---


---

---


---

---

---



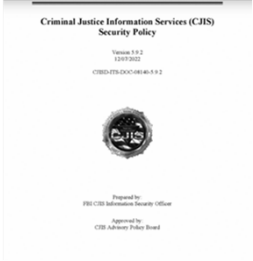
## Criminal Justice Information Services (CJIS) Security Policy



<https://le.fbi.gov/cjis-division/cjis-security-policy-resource-center>

<https://www.fbi.gov/how-we-can-help-you/more-fbi-services-and-information/compact-council>

CJIS Security Policy or CJISSECPOL is minimum set of security requirements for access to FBI CJI.



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)

5

---

---

---


---

---


---

---

---



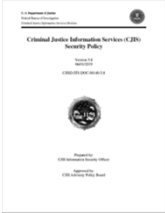
## Minimum Standard Requirement for CJIS Security Policy



Guidance for the implementation of the CJIS Security Policy requirements in the areas of:

- Agency User Agreements
- Local Agency Security Officer (LASO) Appointment
- Awareness and Training (all personnel with access to CHRI)
- Personnel Security
- Media Protection
- Physical Protection
  - Physically Secure Location or Controlled Area
- Incident Response
- Secondary Dissemination (when allowed)

The FBI CJIS Security Policy is updated annually.



6

---

---

---


---

---


---

---

---



### Michigan Addendum to the FBI CJIS Security Policy



The Michigan Addendum to the FBI CJIS Security Policy, hereafter referred to the Michigan Addendum or Addendum, must be read in conjunction with the Michigan CJIS Administrative Rules when interpreting and applying its provisions.

The Michigan Addendum applies to every individual (contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity) with access to, or who operates in support of, criminal justice services and information.

7

---

---


---

---


---

---

---



### Triennial Compliance Audit Reviews



**5.11.1.1 Triennial Compliance Audits by the FBI CJIS Division**

- Conducts audits at a minimum of once every three (3) years to ensure agency compliance with applicable statutes, regulations, and policies.

**5.11.2 Audits by the CJIS Systems Agency**

- In Michigan, the CSA is the MSP.
- Establishes a process to periodically audit all NCJAs with access to CJJ, including CHRI which is a subset of CJI.

8

---

---


---

---


---

---

---



### Triennial Compliance Audit Reviews



- FBI Information Technology Security Audit (ITSA) Review**
  - Assess agency compliance with FBI CJIS Security Policy for CJI in areas of storage, and access. Basically an evaluation of policy and procedure governing the technical security of CJI.
- FBI Next Generation Identification (NGI) Audit Review**
  - Evaluates compliance with applicable laws, regulations, policies, rules, and procedures. Ensures system integrity.

9

---

---


---

---


---

---

---




### Auditor Map



NCJA Region	Local Agency Name	Local Agency Address	Local Agency Phone	Local Agency Email
1	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
2	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
3	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
4	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
5	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
6	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
7	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
8	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
9	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
10	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
11	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
12	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
13	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
14	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
15	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
16	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
17	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
18	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
19	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
20	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
21	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
22	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
23	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
24	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
25	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
26	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
27	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
28	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
29	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
30	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
31	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
32	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
33	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
34	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
35	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
36	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
37	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
38	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
39	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
40	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
41	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
42	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
43	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
44	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
45	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
46	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
47	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
48	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
49	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
50	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
51	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
52	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
53	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
54	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
55	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
56	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
57	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
58	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
59	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
60	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
61	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
62	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
63	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
64	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
65	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
66	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
67	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
68	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
69	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
70	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
71	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
72	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
73	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
74	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
75	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
76	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
77	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
78	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
79	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
80	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
81	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
82	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
83	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
84	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
85	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
86	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
87	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
88	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
89	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
90	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
91	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
92	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
93	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
94	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
95	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
96	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
97	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
98	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
99	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov
100	Alcona	1000 N. 1st St.	617-249-0953	DavisR40@michigan.gov

Blue: Robert Davis  
517-249-0953  
DavisR40@michigan.gov

Green: Lori Higgins  
517-614-9328  
HigginsL2@michigan.gov



10

---

---

---


---

---


---

---

---



### Local Agency Security Officer (3.2.9)



**LASO – designated by the NCJA:**

- Identify who is accessing CHRI
- Identify how the NCJA is connected to CHRI
- Ensure security measures are in place and working
- Support policy compliance and ensure the reporting of any CHRI incident to the MSP Information Security Officer (ISO)
- Review agencies CHRI policy annually or after security events

11

---

---

---


---

---


---

---

---



### Local Agency Security Officer (3.2.9)



Employ one or more of the following techniques to increase the security and privacy awareness of system users:

- Displaying posters
- Offering supplies inscribed with security and privacy reminders
- Displaying logon screen messages
- Generating email advisories or notices from organizational officials
- Conducting awareness events

12

---

---

---

---

---

---

---

---

## Local Agency Security Officer (3.2.9)

LAJIS-015 (03/2015)  
 Michigan State Police  
 Criminal Justice Information Center

ADDITIONAL: VOLS 28-214 and VOLS 28-162  
 COMPLIANT: Michigan, Indiana, Nevada  
 (Michigan Vol. 28-214 is a part of Request)

NONCRIMINAL JUSTICE AGENCY  
 APPOINTMENT NOTIFICATION

All Noncriminal Justice Agencies (NCJAs) that have access to Criminal Justice Information (CJIS), a subset of Criminal Justice Information, shall appoint a security point of contact known as a Local Agency Security Officer (LASO). The LASO can be, but is not required to be, the NCJA department head (e.g., superintendent, president, director, etc.).

All NCJAs that also have access to the Criminal Justice Information System (CJIS) are required to appoint a CHERISS Administrator to be the contact for access to CHERISS.

In design to appointment of the LASO and/or CHERISS Administrator must be reported to the Michigan State Police, Criminal Justice Information Center by returning this completed form through one of the methods listed below. The LASO and CHERISS Administrator may be the same person.

Note: Submitting this form makes no guarantee. All current LASOs and CHERISS Administrators of a work site who are not listed on this form will lose their administrative rights immediately.

**Send Completed Form To:**  
 Michigan Department of State Police  
 Criminal Justice Information Center  
 ATTN: Security and Access Section  
 P.O. Box 30044 Lansing, MI 48909-0434  
 OR E-mail: [SECURITY@MichiganStatePolice.org](mailto:SECURITY@MichiganStatePolice.org)  
 OR Fax: 517-373-0155

**For Additional Information:**  
 (800) 662-2262  
 (517) 373-0155  
 Phone: 517-373-0155

I. Agency Information			
Agency Name	Agency ID	Agency Phone	Agency Fax
Agency Address	City	State	Zip
II. Appointment Information			
Appointee Name (First Name, Last Name, MI):			
LASO		Phone	Fax
CHERRIS Administrator		Phone	Fax
III. Approval			
Principal of Agency Head and Title:			

This form is available for agency's use and can be found at the following link: [www.michigan.gov/cjiscts](http://www.michigan.gov/cjiscts) (Forms).

13

## Awareness and Training (5.2)

All users with authorized access to CJIS should be made aware of their individual responsibilities and expected behavior when accessing CJIS and the systems which process CJIS.

- part of initial training for new users **prior** to accessing CJIS
- annually thereafter
- when required by system changes
- within 30 days of any security event for individuals involved in the event.

LASOs require enhanced training on the specific duties and responsibilities of those positions and the impact those positions have on the overall security of information systems.

TODAY'S TRAINING IS NOT SECURITY AWARENESS TRAINING

14

## Awareness and Training (5.2)

### Role-Based Training

**Unescorted Access to Secure Locations:**

- **Basic Role** - (previously known as Level 1): Personnel with Unescorted Access to a Physically Secure Location. This level is designed for people who have access to a secure area that contains Criminal Justice Information (CJIS) but are not authorized access to CJIS. Examples would be building maintenance and janitorial personnel. This is not common for NCJA using a controlled area.

**Access to CJIS:**

- **General Role** - (previously known as Level 2 and Level 3a/b): All personnel with access to CJIS. This level is designed for people who have physical and logical access to CJIS. Previously this training was split between those that have access to physical (paper copies) only and those that have access to both physical and logical (computer systems) CJIS. The FBI has combined the two modules into General Users. Examples would be all law enforcement officers, dispatchers, court clerks, etc.


**CHERRIS Admin:**

- **Privileged Role** - (previously known as Level 4): Personnel with information technology roles. This level is designed for all information technology personnel including system administrators, security administrators, network administrator, etc. More access needed than a general user, but not an assigned LASO.


**LASOs:**

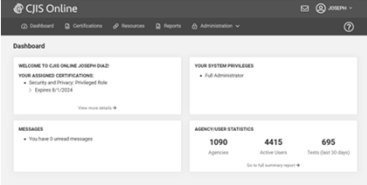
- **Security Role** - "Organizational Personnel with Security Responsibilities" (previously known as Enhanced Security Training for LASOs): This level is designed for personnel with the responsibility to ensure the confidentiality, integrity, and availability of CJIS and the implementation of technology in a manner compliant with the CJISSECPOL - LASOs

15



# CJIS Online





The Michigan State Police (MSP) is pleased to introduce the new CJIS Online training platform to deliver the Federal Bureau of Investigation (FBI) CJIS Security Policy (CJISSECPOL) required Awareness and LASO Training. The new platform is a commercial off-the-shelf web-based product currently in use by 42 states and more than 10,000 vendor companies with the following attributes:

- Available at no cost to your agency.
- Compliant with CJISSECPOL requirements.
- Administrators will have the ability to manage and track learner accounts and records.
- Administrators and learners will receive notifications when retraining is required.
- Local administrators will have access to vendor training records as well as online access to vendor Security Addendums for more than 10,000 vendor companies across the nation.

---

---

---

---

---

---

---

---

16





# Questions?

---

---

---

---


---

---


---

---

17



# Federal Authorities (not all inclusive)



- National Child Protection Act and Volunteers for Children Act (NCPA/VCA) – Must have a state law for use.
- Adam Walsh Child Protection and Safety Act (AWA)
- Serve America Act (SAA)
- Real ID Act
- Housing Opportunity Program Extension Act
- Private Security Officer Employment Authorization Act
- Nursing Facility/Home Health Care Agency Act
- Violence Against Women Reauthorization Act
- Affordable Care Act, Sections 6201 and 6401
- Commercial Motor Vehicle Safety Enhancement (CMVSE) Act
- Indian Child Protection & Family Violence Prevention Act
- 92-544 laws – Must have a state law for use.

---

---

---

---

---

---

---

---

18

19

20

21



---

---

---

---

---

---

---

---

---

---

---

---

8





## Fingerprint Consent

**USE SCAN FINGERPRINT BACKGROUND CHECK REQUEST**

**Consent**

**Live Scan  
Fingerprint  
Background Check  
Request  
(RI-030)**

28

---

---

---

---

---

---

---

---

## Fingerprint Consent

**I. Authorizing Information**

1. Fingerprint Reason Code  2. Requestor/Agency ID  3. Agency Name  4. Individual ID (MNU-OA)

**II. Applicant Information:** Type or clearly print answers in all fields before going to be fingerprinted.

1a. Last Name  1b. First Name  1c. Middle Initial  1d. Suffix

2. Any Alternative Names, Last Names, or Aliases  3. Social Security Number (Optional)

4. Place of Birth (State or Country)  5. Date of Birth  6. Phone Number  7. Driver's License / State ID Number  8. Issuing State

9. Home Address  10. City  11. State  12. ZIP Code

13. Sex  14. Race  15. Height  16. Weight  17. Eye Color  18. Hair Color

**III. Live Scan Information**

1. Date Printed  2. Picture ID Type Presented  3. Transaction Control Number (TCN)  4. Live Scan Operator\*

\*When an individual ID is provided, please enter the ID into the Miscellaneous Number (MNU) field on the Live Scan device. Select OA - Originating Agency Identifier and then enter the unique identifier in the Identification Code field.

29

---

---

---

---

---

---

---

---

## Fingerprinting Procedures

- School Employment (SE)** – Is used for the fingerprinting of an applicant or an individual who is hired for any full-time or part-time employment, or who is assigned to regularly and continuously work under contract in any of its schools. Applicants or individuals working or assigned in this capacity are required to have a fingerprint-based background check. A school may also choose to fingerprint a person employed by, or seeking to be employed with, the school for a position that is not covered within the Revised School Code. SE fingerprinting may be used for person paid by the school in any non-K-12 position who have, or may have, unsupervised access to a child whom the school provides care, treatment, education, training, instruction, supervision, or recreation. (i.e., such as a community swim lifeguard or school established childcare program employees, etc.)
- School Volunteer (SV)** - Is used for any individual solicited to provide a volunteer service providing care to the school's vulnerable population.

30

---

---

---

---

---



---

---


---

[illegible]


# Position Documentation



- Position documentation for the fingerprint reason code used by the agency - documentation which indicates the fingerprint-based CHRI background checks obtained are for a specific purpose authorized by state or federal law - examples:
  - Tentative offer letters
  - Hiring documents used consistently for all employees
  - Volunteer forms
  - The Michigan Waiver Agreement & Statement form for NCPA/VCA fingerprints (mandatory for NCPA/VCA)



# Applicant Appeal Process



Written  
instructions  
with a time  
frame

Applicants may share CHRI with an applicant for the purpose of challenge, correction, or update.

Prior to release, the applicant must determine through picture ID that applicant and record (CHRI response) are "one in the same."

Can include the state and federal portion of CHRI.

**Agency Appeal Process**

**AGENCY NAME** \_\_\_\_\_

**AGENCY RESPONSE** \_\_\_\_\_

**RE:** \_\_\_\_\_

*Original Request Received: Information Challenge or Correction*

Pursuant to federal statute, individuals may challenge the accuracy or completeness of any records on the Commission's Representative Information (CHRI) response received. Applicants wishing to challenge or update their request must:

- Request an appointment with the living Person(s) Tied to the CHRI(s) of the challenging CHRI response within the 60-day time frame of the CHRI response.
- Be given (or given to) the living Person(s) tied to any questioned information within the record.

Applicants must be given an opportunity to meet with the living Person(s) tied to any questioned information within the record. If unable to meet, applicants must be given the opportunity to meet with the Commission's representative. This opportunity must be given within 60 days of the CHRI response.

Any challenge or update request must be received by the applicant's living Person(s) within 60 days of the CHRI response. If the challenge or update request is not received within 60 days, the challenge or update request will be considered as the decision of the agency (CHRI).

If you are unable to receive the information update through this method, you may contact us at:

**Out of State Request**

Call toll-free and make appointments to the FBI Criminal Justice Information Center (CJIC), Detroit, MI. Our Commission's website is: [www.fbi.com](http://www.fbi.com) or 1-800-254-3431. For more information, visit the FBI website for more details: <https://www.fbi.com/services/records-services>. Subsequent to the meeting, the Commission will provide a written response to the challenge or update request.

**In State Request**

Challenge requests to Michigan State Police are to be made at 2144 Kalamazoo Ave. in Grand Rapids, MI. For more information, visit the Commission's website: [www.michigan.gov](http://www.michigan.gov) or 1-800-254-3431. For more information, visit the Commission's website: [www.michigan.gov](http://www.michigan.gov).

**As the applicant's challenge or update request is received, it is your responsibility to keep (your) Identification of all persons being challenged.**

Upon successful completion of a challenge or update, the applicant may request the Michigan State Police's Commission's website is: [www.fbi.com](http://www.fbi.com) or 1-800-254-3431. For more information, visit the FBI website for more details: <https://www.fbi.com/services/records-services>.


I, \_\_\_\_\_, understand and agree to the terms and conditions outlined. I will keep the information contained in the CHRI response and any update request confidential to the person(s) listed. Further, I will not release the information contained in the CHRI response and any update request to any third party without the written approval of the Michigan State Police.

Signature: \_\_\_\_\_ Date: \_\_\_\_\_


34

35

36



### Personnel Screening (5.12.1)



- If a felony conviction of any kind exists, the NCJA Agency shall deny access to CJI. However, the NCJA Agency may ask for a review by the CSO in extenuating circumstances where the severity of the offense and the time that has passed would support a possible variance.
- Applicants with a record of misdemeanor offense(s) may be granted access if the CSO, or his or her designee, determines the nature or severity of the misdemeanor offense(s) do not warrant disqualification. The NCJA Agency may request the CSO review a denial of access determination. This same procedure applies if the person is found to be a fugitive or has an arrest history without conviction.

37

---

---

---


---

---


---

---

---



### Personnel Screening (5.12.1)



- If the person appears to be a fugitive or has an arrest history without conviction, the CSO or his/her designee shall review the matter to determine if access to CJI is appropriate.
- If the person already has access to CJI and is subsequently arrested and or convicted, continued access to CJI shall be determined by the CSO. This does not implicitly grant hiring/firing authority with the CSA, only the authority to grant access to CJI. For offenses other than felonies, the CSO has the latitude to delegate continued access determinations to his or her designee.
- If the CSO or his/her designee determines that access to CJI by the person would not be in the public interest, access shall be denied, and the person's appointing authority shall be notified in writing of the access denial.

38

---

---

---


---

---


---

---

---



### Media Protection (5.8)



NCJAs shall have established policy and procedures for the appropriate security, handling, transporting, and storing of CHRI media. Each NCJA shall establish the following:

- An overall digital/physical media protection policy.
- Procedures restricting access to authorized user/personnel. Management controls are to exist for the processing and retention of CHRI media and for media to be secured in a controlled area.
- Non-Governmental VECHS Agencies only VIEW in CHRISS no physical storage allowed.
- Procedures for transporting CHRI media from its original secured location to another. The steps taken to protect and prevent the compromise of the data in transit. Marking of the media.
- Procedures for the appropriate disposal and sanitization of CHRI media when no longer needed, and the specific steps taken to protect and prevent CHRI media during the destruction process. All destruction is to be logged or documented.

39

---

---

---



---

---

---

---

---

### Physical Protection (5.9)

NCJAs shall establish and implement physical protection policy procedures to ensure CHRI and information systems are physically protected through access control measures. When an agency cannot meet all the control requirements for a physically secure location, the agency shall review and adhere to 5.9.2 – Controlled Area, which states the following:

- Limit access in controlled area during CJ/CHRI processing times
- CHRI room or storage area should always be locked when not in use
- Position CHRI to prevent unauthorized individuals from access and view
- Agencies shall carry out encryption requirements for digital storage of CHRI
  - At rest: Advanced Encryption Standard (AES) algorithm and 256-bits
  - In transit: Federal Information Processing Standard (FIPS) 140-2 certified

40

---

---

---



---

---

---

---

---

### Incident Response (5.3)

Each NCJA shall establish operational incident handling policies and procedures for instances of an information security incident of physical/digital CHRI media. Agencies are to ensure general incident response roles and responsibilities are included within the agency established and administered SAT. Each NCJA shall establish:

- Reporting procedures outlining who to report to upon discovery of any incident pertaining to CHRI. Must report to agency LASO within 1 hour.
- Incident handling capability procedures that include adequate preparation, detection, analysis, containment, eradication, recovery, and user response activities.

41

---

---

---



---

---

---

---

---

### Incident Response (5.3)

Electronic and Physical Incident Handling Capability Procedures include:

- Preparation – firewalls, virus detection, malware/spyware detection, security personnel, and locked doors to prevent unauthorized access.
- Detection – monitoring preparation mechanisms for intrusions such as: spyware, worms, and unusual or unauthorized activities, etc. Can include building alarms and video surveillance.
- Analysis – identify how an incident occurred and what systems or CHRI media were compromised.
- Containment – security tools utilized or an agency plan to stop the spread of the intrusion.
- Eradication – removal plan of the intrusion before the system is restored and steps taken to prevent reoccurrence.
- Recovery – the ability to restore missing files or documents.

42

---

---

---


---

---


---

---

---



## Incident Response (5.3)



Each NCJA shall establish:

- Procedures for the appropriate collection of evidence, for incidents involving legal action (either civil or criminal) against a person or agency (calling law enforcement or contacting legal counsel).
- Procedures to track, document, and report information security incidents. An Information Security Officer (ISO) Security Incident Report form (CJIS-016). Must be reported LASO immediately not to exceed 1 hour after discovery.
- Agency incident response plan is to includes a process to assessment extent of the harm.
- Test the effectiveness of the plan annually, walk through exercise.

43

---

---

---


---

---


---



---

---



## Incident Response (5.3)



**Information Security Officer (ISO) Security Incident Report (CJIS-016)**

This form is available for agency's use and can be found at the following link: [www.michigan.gov/cjicats](http://www.michigan.gov/cjicats) (Forms).

44

---

---

---


---

---


---

---

---



## Secondary Dissemination (5.1.3)



The NCJA is required to obtain written consent from the individual for any request for secondary dissemination of CHRI conducted outside the primary information exchange agreements and are to be logged using the following:

- The date record was shared
- Who made the request
  - Requesting Agency
  - Recipient Name
- Whose record is being shared
- Who sent the shared copy (personnel)
- How the request was fulfilled

A Secondary Dissemination template is available for agency's use and can be found at the following link: [www.michigan.gov/cjicats](http://www.michigan.gov/cjicats) (Templates).

45

---

---

---

---

---

---

---

---






Questions?

46

---

---

---



---

---

---

---


---

### How an Agency is Chosen for Audit

The following Triennial Audit Cycles have included Noncriminal Justice Agencies:

- 2010-2013
- 2013-2016
- 2016-2019
- 2019-2022
- 2022-2026 – Current Cycle**



"We're going to parachute in and do a surprise audit, but I want to keep the whole thing low key."

- Auditors plan their next entire year of audits at the end of the current year.
- Agencies are chosen by region and may include State of Michigan agencies, nonpublic schools, public schools, public school academies, local government agencies, and public entities such as colleges and local municipal entities.

47

---

---

---



---

---

---

---

---

### NCJA Compliance Audit Review Notification

A NCJA will receive an email notification from your auditor to the point of contact for the agency. The notification will include:

- Date and time of your agency audit
- An attached random fingerprint sample of 20 individuals fingerprinted under your agency ID over last year
- Request for acknowledgement and address confirmation
- Instructions for logging in to the MSP CJIS Portal and completing the online NCJA Pre-Audit Questionnaire
  - This will include a Username
  - Your password will be emailed in a separate email to follow

48

---

---

---

---


---

---


---


---






## Pre-Audit Questionnaire





Michigan State Police



Agency Login

FullAdmin Login

Launch Help Page

powered by  
Blue Technology Solutions

**MSP CJIS Portal** – <https://michigan.cjisapps.com/cjisaudit/index.pl>

- NCJA Audit Review
  - Required
- NCJA Technical Security Audit Review
  - Only required if agency is storing CHRI digitally on its system
  - Not required for CHRIS storage
  - This will be sent separately if an agency is determined to be storing electronic CHRI

---

---

---

---


---

---


---

---

49



## Pre-Audit Questionnaire Supporting Documents



- All supporting documents required for the audit are now able to be uploaded into the Pre-Audit Questionnaire.
- Providing the requested files and documentation prior to the auditor's arrival provides an opportunity to complete the onsite visit in a timely manner.

---

---

---

---


---

---


---

---

50



## Draft Audit Report Notification



- Within 15 business days of your audit, the auditor will send you an email that includes instructions to log back into the audit tool where you completed the pre-audit questionnaire.
- You will have 30 days to respond.

Dear [Name],

A draft compliance audit report is ready for your review within the Michigan State Police (MSP) Criminal Justice Information Services (CJIS) Audit Portal for the Noncriminal Justice Agency Use of Criminal Justice Information Audit conducted on [Date]. This was a compliance audit review conducted to determine the proper use, storage, and dissemination of criminal history record information [1]. The compliance report includes, if applicable, instances of noncompliance identified during the on-site audit by the MSP auditor.

The auditor respectfully requests an agency response by Date: [Date], which includes your agency's proposed plan for corrective action(s) concerning the out of compliance areas. This response is to be submitted through the MSP CJIS Audit portal at <https://www.cjisportal.com/NCJISaudit/index.pl> (<https://www.cjisportal.com/NCJISaudit/index.pl>). Once logged into the CJIS Audit Portal:

- Click the "Response Required" button. The compliance report will load showing the out of compliance findings from the compliance audit.
- Then click on the "Add button" and provide your agency's proposed plan for corrective action(s) for each area found out of compliance and a timeframe in which it will be implemented.
- Once all of your agency responses are entered, click "Save for Final Review".

Please do not copy and paste any additional supporting documentation regarding your agency's corrective action into your response, but forward it to [audit@michigan.gov](mailto:audit@michigan.gov). If your agency is not able to respond in the allotted time provided, contact our office at once to discuss your agency's options and concerns with the auditor. Formal request for a response extension can be sent to your auditor, and is to include the following:

- Request for an extension.
- Purpose for the delay of the response.
- Contact information for the agency representative making the request.

---

---

---

---

---

---

---

---

51



## Tools for a Successful Audit



52

---

---

---


---

---


---

---

---



## CJIS CSO Referral



Assessed Area	Issue
NIS	Improper use of fingerprint reason code
NIS	Dissemination to unauthorized recipients
NIS	Outsourcing
NIS	Lack of Agency User Agreement
NIS	Lack of supporting documentation for reason fingerprinted (more than 9.5% of records assessed)
IT	Lack of encryption: <ul style="list-style-type: none"> <li>In transit</li> <li>At rest</li> </ul>
IT	Lack of proper user authentication: <ul style="list-style-type: none"> <li>Used ID (proper name, dictionary word, etc.</li> <li>Missing required attributes (identify which one)</li> </ul>
IT	Lack of required policies: <ul style="list-style-type: none"> <li>Incident response</li> <li>Personnel termination</li> </ul>
IT	System integrity: <ul style="list-style-type: none"> <li>Lack of required patch management</li> <li>Lack of malicious code protection</li> <li>Lack of spam and spyware protection</li> </ul>
IT	Physical security – no controlled area for processing CHRI
GEN	Failure to participate in audit
GEN	Failure to provide corrective action for out of compliance findings

NIS = National Identity Services

IT = Information Technology

53

---

---

---


---

---


---

---

---



## Resources and Tools





Please visit our website to obtain:


- Forms
- Templates
- Guidance
- Audit & Training Information


MSP Security & Access Website:  
[www.michigan.gov/cjicats](http://www.michigan.gov/cjicats)


**Templates**


• **NICAD Security Awareness Training Template (PowerPoint Presentation)**    
 A template for a NICAD user. Agencies are responsible to customize the Security Awareness Training (SAT) to fit their agency's needs. It is required by the FBI CAD Security Policy (June 2012). The SAT Template is a file in PowerPoint to be completed by the agency prior to administering.


• **Background Information Log**    
 A template for a NICAD to use in any instance where a Criminal History Record Information (CHRI) response is shared with another qualified entity outside the original request.

• **Provisional Background Check**    
 A template for a NICAD to use as representation of supporting documentation "Provisional Description" for valid purposes when requesting fingerprint (agencies by state or federal statute) or conducting an Internal Criminal History Review (ICHR) same search, on volunteers of the agency. Provisional Description is the performance of the fingerprint request.

• **Documentation for Assignment**    
 A template for a NICAD user. Commonly referred to as a red lightgreen light notification and is to be used when the agency is offering a contract for individual assigned to register and continuously work under contract in a K-12 school education position.

• **Consent to Share**    
 A template for a NICAD to be used in an instance where the agency is not going to share a CHRI response with another qualified entity.

• **Agency Support Process**    
 A template for a NICAD user in order to meet the federal requirement. A NICAD in receipt of CHRI is required to establish policy and procedures to ensure the appropriate security and management controls necessary.

• **NICAD Information Security Policy**    
 A template for a NICAD user in order to meet the federal requirement. A NICAD in receipt of CHRI is required to establish policy and procedures to ensure the appropriate security and management controls necessary.

Forms

Guidance

Audit

54

---

---

---



---

---

---

---

---





Questions?

55

---

---

---

---

---

---

---



THANK YOU !!!!!

For your time and attention.  
We look forward to working with you in the future.

56

---

---

---

---

---

---

---