

Federal Bureau of Investigation  
Criminal Justice Information Services  
Security Policy

Michigan Addendum to the FBI Criminal Justice Information Services Security Policy  
(May 28, 2021)

The Michigan Addendum to the Federal Bureau of Investigation (FBI) Criminal Justice Information Services Systems Security Policy, hereafter referred to the Michigan Addendum or Addendum, must be read in conjunction with the Michigan Criminal Justice Information Systems (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.

DEFINITIONS:

As used in the Michigan Addendum:

- A) "Convicted" means a final conviction, the payment of a fine, a plea of guilty or nolo contendere if accepted by the court, or a finding of guilt for a criminal law violation.
- B) "Criminal Justice CJIS User Agency" (CJCUA) is an agency authorized to access Criminal Justice Information (CJI) pursuant to R 28.5201(1)(a) and (c) of the Michigan CJIS Administrative Rules.
- C) "Criminal justice information" (CJI) is as defined in the FBI CJIS Security Policy and the Michigan CJIS Administrative Rules.
- D) "Direct Access" means having the ability to query or update CJIS, whether by manual or automated methods, not requiring the assistance of, or intervention by, any other party or agency.
- E) "Non-Criminal Justice Agency" (NCJA) is an agency authorized to access CJI that is criminal history record information for civil purposes pursuant to a state statute approved by the FBI, or federal law.
- F) "Non-Criminal Justice CJIS User Agency" (NCJCUA) is an agency authorized to access CJI pursuant to R 28.5201(1)(b), (d), (e), and (f) of the Michigan CJIS Administrative Rules.

POLICY TOPIC: CJIS Systems Officer (CSO) Policy Regarding "Access"

Reference: 3.2.2.2

Date: May 28, 2021

Access includes all individuals with unescorted access to unencrypted CJI. This includes all authorized users and those individuals responsible for configuring and maintaining computer systems and networks with access to or containing CJI.

POLICY TOPIC: Applying FBI Criminal Justice Information Services Security Policy to Agencies with Michigan-Only Access

Reference: Entire FBI Criminal Justice Information Services Security Policy

Date: October 26, 2012, revised July 14, 2017, revised May 28, 2021

POLICY:

All agencies with access to CJI provided via the Michigan State Police shall abide by current FBI Criminal Justice Information Services Security Policy and this addendum.

POLICY TOPIC: CJIS System Agency (CSA) Information Security Officer (ISO)  
Reference: 3.2.8 (4)  
Date: October 26, 2012, revised July 14, 2017, revised May 28, 2021

POLICY:

When investigating an incident that significantly endangers the security or integrity of CJI or CJIS, the Local Agency Security Officer (LASO) shall complete and submit an Information Security Officer (ISO) Computer Security Incident Report form (CJIS-016) to the ISO.

POLICY TOPIC: Local Agency Security Officer (LASO)  
Reference: Date: 3.2.9  
Date: October 26, 2012, revised July 14, 2017, revised May 28, 2021

POLICY:

Each agency having access to CJI shall establish an information security structure that provides for a LASO. The LASO shall ensure and oversee the management of encryption between the CJIS User Agency and its users and shall be a Point of Contact (POC) in the event of an attempted security breach of the CJIS network. The LASO may act as POC for nonterminal and noncriminal justice agencies.

POLICY TOPIC: Visitor Control  
Reference: 5.9.1.7  
Date: October 26, 2012, revised May 28, 2021

POLICY:

A visitor is defined as any individual who is not authorized unescorted access to a physically secure location and whose documented record of entry into the physically secure location could not adversely impact investigations (e.g., confidential informants, witnesses, victims, etc.).

POLICY TOPIC: Facsimile Transmission of Criminal Justice Information  
Reference: 5.8 and 5.10.2  
Date: October 26, 2012, revised July 14, 2017, revised May 28, 2021

POLICY:

When transmitting CJI via a facsimile (FAX) machine to a non-physically secure location, the sender shall notify the intended recipient prior to the transmission. CJI shall only be sent to a non-physically secure location when it is confirmed that the intended recipient is immediately available to receive and secure the information.

POLICY TOPIC: Audits by the CSA  
Reference: 5.11.2  
Date: October 26, 2012, revised July 14, 2017, revised May 28, 2021

POLICY:

The CSO reserves the right to conduct a security and/or compliance audit on any agency or contractor with access to CJI.

POLICY TOPIC: Personnel Security Policy and Procedures

Reference: 5.12.1

Date: October 26, 2012, revised July 14, 2017, revised May 28, 2021

1. POLICY:

- A) Each User Agency shall develop and maintain a written personnel screening policy and procedure detailing the User Agency's criteria for approving and denying access to CJI, which shall include all users and those individuals responsible for configuring and maintaining computer systems and networks with access to or containing CJI. The policy and procedure shall include the minimum standards set forth in this addendum and whether to deny access for misdemeanor convictions. CJCUIAs and NCJCUIAs shall also include whether to deny access for records deferred under the statutes listed in the table below. A User Agency's policies and procedures shall not be less strict than the FBI Criminal Justice Information Services Security Policy and this addendum.

MCL	General Description
333.7411	Controlled Substance (7411)
436.1703	Minor in Possession (MIP) of Alcohol
769.4a	Domestic Violence (ABUSE)
762.14	Holmes Youthful Training Act (HYTA)
750.451c	Human Trafficking Victim Protection
750.430	Practicing under the Influence (HEAL)
600.1076	Drug Treatment Court (DTCT)
600.1095	Mental Health Court (MHC)
600.1209	Veterans Court (VET)
750.350a	Parental Kidnapping (KID)
780.623	Conviction Set Aside (adult)
712A.18e	Adjudication Set Aside (juvenile)

- B) The CSO authorizes User Agencies to approve individual access to CJI in accordance with the FBI Criminal Justice Information Services Security Policy and this addendum. The CSO reserves the right to deny or revoke access to CJI when access by the person would not be in the public interest.
- C) Upon initial request for access to CJI, the User Agency shall comply with the following:
1. If a conviction for a crime punishable by more than one year exists, access to CJI shall be denied. A CJCUIA or NCJCUIA employee with such a conviction is exempt from this denial if the conviction and the employment occurred prior to March 1, 2001, and the person has maintained continuous employment with the same CJCUIA or NCJCUIA since that time. An NCJA employee with such a conviction is exempt from this denial if the conviction and the employment occurred prior to November 1, 2020, and the person has maintained continuous employment with the same NCJA since that time.
  2. If a misdemeanor conviction involving the misuse of CJI has occurred in the previous one year, access to CJI shall be denied. If two or more misdemeanor convictions involving the misuse of CJI have occurred, access to CJI shall be denied.

3. If the person is found to be the subject of an outstanding arrest warrant, access to CJI shall be denied. The person may be afforded the opportunity to satisfy the warrant, at which time, access to CJI may be re-evaluated.
  4. If the person has an arrest history without conviction or dismissal, review the matter to determine if access to CJI is appropriate.
  5. If access to CJI by the person would not be in the public interest, access shall be denied.
- D) For existing personnel who have access to CJI, the User Agency shall comply with the following:
1. If a conviction for a crime punishable by more than one year occurs, access to CJI shall be revoked.
  2. If a misdemeanor conviction involving the misuse of CJI occurs, direct access to CJI shall be suspended for no less than 90 days. If a subsequent conviction involving the misuse of CJI occurs, access to CJI shall be revoked.
  3. If the person is found to be the subject of an outstanding arrest warrant, access to CJI shall be suspended. The person may be afforded the opportunity to satisfy the warrant, at which time, access to CJI may be re-evaluated.
  4. If the person has an arrest history without conviction or dismissal, review the matter to determine if access to CJI is appropriate.
  5. If continued access to CJI by the person would not be in the public interest, access to CJI shall be revoked.
  6. If access to CJI is or is required to be revoked or suspended pursuant to paragraphs 1-5 above, the CSO shall be immediately notified in a manner prescribed by the CSO.
  7. Revocation or suspension of access to CJI does not require agencies to remove access to an individual's electronic mail account.
- E) The User Agency may ask for a review by the CSO in extenuating circumstances where the severity of the offense and the time passed would support a possible variance.
- F) Where Michigan has not passed state legislation authorizing or requiring civil fingerprint-based background checks, NCJA employees who require access to Criminal History Record Information (CHRI) shall be screened through the Michigan State Police Internet Criminal History Access Tool (ICHAT) prior to accessing CJI. NCJAs are strongly encouraged to screen employees using additional sources, which may include:
- The Michigan Department of Corrections Offender Tracking Information System (OTIS)
  - The Public Sex Offender Registry (PSOR)
  - A local criminal record check (where a person has resided during the previous five years) through a court and/or law enforcement agency
  - Out of state equivalents to ICHAT, OTIS, and PSOR (if available) if the employee resided in another state during the previous five years

G) A NCJCUA shall screen personnel for individual access to CJJ by running/requesting a query through the Law Enforcement Information Network (LEIN) of the Michigan Criminal History Record system. NCJCUAs are authorized to conduct/request additional queries through LEIN of the following:

- Michigan Hot files
- Michigan Department of State driving history
- Michigan personal protection orders
- Michigan Department of Corrections
- Michigan Sex Offender Registry

APPROVED BY: Col. Joseph M. Gasper, May 28, 2021