Reviewed: 02/01/2024

WISCONSIN

TIME SYSTEM

2024 INSERVICE TRAINING

Table of Contents

CJIS Security Policy Changes

The newest update to the CJIS Security Policy was published September 14, 2023. The FBI will continue revising and updating the policy section by section as well as adding new sections over the next couple of years. The FBI estimates that there will be two policy updates per year while this process is ongoing, with the final update to version 6.0 anticipated for Spring 2025. The beginning of the policy overhaul began on October 1st, 2022, with version 5.9.1 and there have been two additional updates since then.

5.9.1 Updates:

This first update focused on modernizing the Media Protection (MP) section of the policy. The new format for the policy provides a topic and security controls for the topic in each section detailing the requirements for the topic. There are six controls for Media Protection with requirements for each control. Each control has a discussion section where more information is provided for the control area. The Media Protection section became sanctionable October 1st, 2023.

Media policy and procedures must be reviewed at least annually and following any security incidents involving digital and/or non-digital media.

Agencies must:

- Restrict the use of digital media and non-digital media on agency-owned systems that have been approved for use in the storage, processing, or transmission of CJI by using technical, physical, or administrative controls.
- Prohibit the use of personally owned digital media devices on all agency owned or controlled systems that store, process, or transmit CJI.
- Prohibit the use of digital media devices on all agency-owned or controlled systems that store, process, or transmit CJI when such devices have no identifiable owner.

Section 5.12 Personnel Security and Appendix G.3 Cloud Computing – This version includes the CJIS Advisory Policy Board's Interpretive Guidance Task Force recommendations on cloud service offerings and guidance related to personnel screening of cloud service personnel.

5.9.2 Updates:

The second update was released December of 2022 and there were a lot of updates to the policy, with some updates being sanctionable October 1st of 2023 and some October 1st, 2024. The sections that were updated were: Identification and Authentication (IA), System and Information Integrity (SI) and Awareness Training (AT).

Awareness and Training (AT) – Security awareness will now be required annually. This change became sanctionable October 1st, 2023, so the biennial recertification alone will

not meet the requirements. Users will have to complete the Security Awareness training every year. The update to Awareness and training also discussed role-based training (general user, privileged user, personnel with security responsibilities).

Identification and Authentication (IA) is a new policy requirement that is sanctionable October 1st, 2024. Agencies will be required to:

- Implement multi-factor authentication for access to privileged and non-privileged accounts.
- Implement replay-resistant authentication mechanisms for access to privileged and non-privileged accounts.
- Accept and electronically verify Personal Identity Verification compliant credentials.
- Prevent reuse of identifiers for one year.
- Manage individual identifiers by uniquely identifying each individual as agency or non-agency.

System and Information Integrity (SI) is a new policy requirement which became sanctionable October 1st, 2023. Agencies are required to:

- Incorporate flaw remediation guidance.
- Implement signature based malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code.
- Employee integrity verification tools to detect unauthorized changes to software, firmware and information systems that contain or process CJI.
- Automatically update spam protection mechanisms at least daily.

5.9.3 Updates:

The third update since the overhaul was released September 14th, 2023. This version of the policy focused on modernizing the following sections of the policy: Incident Response (IR), Access Control (AC) and Maintenance (MA). These items will be sanctionable October 1st, 2024.

The following are requirements for agencies regarding Incident Response (IR) controls:

- Review policies and procedures annually and following any security incidents.
- Review and update incident response training content annually and following any security incidents involving CJI.
- Provide incident response training on how to identify and respond to a breach, including the organization's process for reporting a breach.
- Test the effectiveness of the incident response capability for the system annually using the following tests: tabletop or walk-through exercises; simulations; or other agency appropriate tests.

- Coordinate incident response testing with organizational elements responsible for related plans.

With regards to the Access Control (AC) section, agencies are required to:

- Review and update policies and procedures annually and following any security incidents.
- Manage accounts by defining and documenting the types of accounts allowed and prohibited for use within the system
    - Specify access authorization and attributes for each account
    - Automatically remove temporary and emergency accounts within 72 hours
    - Require that users log out when a work period has been completed
    - Disable accounts of individuals within 30 minutes of discovery of direct threats to confidentiality, integrity, or availability of CJI.
- Enforce a limit of five consecutive invalid logon attempts by a user during a 15-minute time period.
- Automatically terminate a user session after a user has been logged out.
- Prohibit the use of personally owned information systems including mobile devices (bring your own device [BYOD] and publicly accessible systems for accessing, processing, storing or transmitting CJI.

Maintenance (MA) is a new section of the policy. Agencies are required to:

- Review policies and procedures annually and following any security incidents.
- Control maintenance (who is coming in or which people are remoting in).
- Approve the removal of system components.
- Sanitize equipment being removed and make sure all controls are functioning properly when equipment is returned.
- Approve and monitor the use of system maintenance tools.
- Perform fingerprint-based background checks and security awareness training for maintenance personnel with unescorted access.
- Obtain maintenance support for crucial system components that process, store and transmit CJIS within agency defined recovery time.

The entire policy can be reviewed at CJIS Security Policy Resource Center — LE (fbi.gov). The companion document is also available in the same location, which breaks down each control and the sanctionable date.

National Threat Operations Center (NTOC)

The FBI's National Threat Operations Center (NTOC) has multiple options to allow the public to provide tips that may help protect the nation. NTOC has fielded tips via phone calls, E-Tips through their website (https://tips.fbi.gov), their social media accounts and

from private sector companies. The National Threat Operations Center (NTOC) is operational 24 hours a day, 7 days a week, and 365 days a year. It reviews and processes tips received from the public to determine whether they are related to matters of national or public security to provide criminal justice agencies with the information that they need to protect the public, NTOC relays tip information that they receive to the appropriate agencies via the International Public Safety and Justice Network (Nlets) Administrative Messages. The Administrative message provides agencies real time information enabling agencies can take appropriate action at their discretion. Other processes in place with for tips that contain immediate action.

Below are some examples of tips received by NTOC which may be shared with agencies at the state, local or tribal level:

- Drug related information
- Stalking/harassment complaints
- Suspicious activity/noise complaints
- Burglary/theft reports
- Poisoning complaints
- Missing person reports (no FBI case)
- Tips with personally identifiable information
- Tips with location information

Below is a sample administrative message of an NTOC tip.

AM. DCFBIWAE1
12:30 07/7/2023

TITLE: FBI NATIONAL THREAT OPERATIONS CENTER INFORMATION SHARING

CAVEAT:
THE INFORMATION HEREIN WAS SUBMITTED BY THE PUBLIC, SOCIAL MEDIA OR PRIVATE SECTOR COMPANIES TO THE FBI TIP LINE AND HAS NOT BEEN CONFIRMED, INVESTIGATED, OR VETTED BY THE FBI. THE INFORMATION PROVIDED IS TO BE USED AT THE DISCRETION OF THE RECEIVING AGENCY TO FURTHER ITS LAW ENFORCEMENT FUNCTIONS. YOU ARE RECEIVING THIS MESSAGE BASED ON ZIP CODE MAPPING.

ORI RECIPIENTS: WVX000000 WV2345670 FBIHQ09842
TRANSACTION REFERENCE NUMBER: 1234xyz
SYNOPSIS: CALLER REPORTED SUSPICIOUS ACTIVITY IN THE PARKING LOT OF THE MOVIE THEATRE DOWNTOWN. CALLER STATED HE SAW 5 MEN COME OUT OF A WHITE VAN, ALL HEADED IN SEPARATE DIRECTIONS AND HAD THEIR PHONES OUT. IT APPEARED THEY WERE VIDEOING RANDOM FEMALES IN THE PARKING LOT. WHILE CALLER WAS WALKING INTO WORK, AT THE THEATRE, ONE OF THE MEN HE SAW LEAVE THE VAN WAS FOLLOWING CLOSELY BEHIND A SINGLE FEMALE AND APPEARED TO BE RECORDING HER ON HIS PHONE. THE CALLER RECOGNIZED THE MAN TO BE TIMMY TESTING.
INCIDENT ZIP CODE: 12345
DATE: 7/7/2023
COMPLAINANT:
NAME: TOMMY TESTER
PHONE NUMBER: 222-333-1234
SUBJECT:
NAME: TIMMY TESTING
PHONE NUMBER: 222-333-1235

SOME ADDITIONAL NTOS RELATED DATA, ALONG WITH UNCLASSIFIED CRIMINAL JUSTICE INVESTIGATIVE INFORMATION, MAY BE FOUND IN THE FBI'S NATIONAL DATA EXCHANGE (N-DEX) SYSTEM. THE N-DEX SYSTEM IS A NO COST NATIONWIDE INFORMATION SHARING SYSTEM WITH ACCESS TO OVER ONE BILLION FEDERAL, STATE, LOCAL, AND TRIBAL RECORDS. FOR MORE INFORMATION ABOUT THE N-DEX SYSTEM, PLEASE CONTACT NDEX@LEO.GOV.

For any questions please do not hesitate to reach out to the TIME and Technical Unit at cibtrain@doj.state.wi.us or TSCC at 608-266-7633.

Warrant Service

Recently, CIB staff members have received clarifying questions from field users about the definition of warrant service. One common question is “When is a warrant considered served?” CIB staff cannot give legal advice or opinions. However, state law does provide a clear answer to this question. Wis. Stat. § 968.04(4)(b) specifically states that "A warrant is served by arresting the defendant and informing the defendant as soon as practicable of the nature of the crime with which the defendant is charged."

Therefore, two conditions must be met for a warrant to be considered served:

1) The subject must have been arrested.
2) The subject must have been informed of the warrant and the reason for the warrant.

Both criteria must be met for the warrant to be considered “served”. Why is the answer to this question so important? Once a warrant has been served, it is no longer a valid warrant and as such should not be listed on the TIME System.

So, ask yourself: have both conditions been met? If yes, the warrant has been served, is no longer valid and must be removed from the system. If not, the warrant is still valid.

Scenario 1: A subject calls a local sheriff’s office to find out if there is a warrant for their arrest. After confirming their identity, the subject is notified that there is a warrant out for them. Is this person considered “served” simply by telling them that there is a warrant? No, because they are not under arrest.

Scenario 2: A burglary suspect is taken into custody following an attempted burglary. The individual also has a warrant out for their arrest from a neighboring agency. The officers that have arrested the individual on the burglary charges but have not yet notified the individual of the warrant. So, has the individual been served on the warrant? No, because they have not been notified of the warrant.

Scenario 3: An officer makes a traffic stop on an individual for speeding. When querying the driver, the officer sees there is a warrant for Disorderly Conduct on the individual. After proper hit confirmation procedures are completed with dispatch, the officer takes the driver into custody and notifies them of the warrant for DC. Has this warrant been served? Yes, since both conditions have been met, the warrant is considered “served.”

Please remember that if both conditions are met, that entry must be removed from the TIME system immediately or a locate must be placed on the record.

Record Documentation

Warrant Requirements for Criminal Proceedings:

1. The warrant must be in writing and signed by the judge.
2. It must state the name of the crime and section charged and number of the section alleged to have been violated.
3. It must have a copy of the complaint attached to it.
4. It must state the name of person being arrested, if known. If not known, designate the person to be arrested by any description by which the person to be arrested can be identified with reasonable certainty.
5. State the date when the warrant was issued and the name of the judge who issued it together with the title of the judge's office.
6. The warrant must command that the person against whom the complaint was made be arrested and brought before the judge issuing the warrant or if the judge is absent or unable to act; before some other judge in the same county.
7. The warrant shall be in the format according to the WI State Statute 968.04(3)(b)3a.

Warrant Requirements for Municipal Court:

1. The warrant requires the name of the defendant.
2. The warrant requires a copy of the citation or complaint.
3. The warrant requires a finding of probable cause that the defendant committed the offense.
4. The warrant requires a command to arrest the defendant and bring them before the municipal judge or other municipal judge or judge of the county.
5. The warrant requires the date of issuance.

Once it is verified that all of these requirements have been met, the warrant can be entered into the TIME System.

What must the warrant case file contain?

1. The case file must contain a copy of the warrant to support a wanted person entry. (The copy can be either electronic or a hard copy).

2. The case file must contain any supporting documentation from the TIME System or other sources of information that were included in the entry. Every field must be accounted for. Below are some examples of supporting documentation.
    a. Place of Birth was obtained from III. A copy of the III must be included in the case file.
    b. The agency's RMS had caution / medical conditions. A printout from RMS must be included in the case file.

c. The agency finds a unique tattoo for the individual on their social media profile. The agency must print out a copy of this and include it in the case file.

3. The case file must contain documentation of any supplemental information added to the entry or modifications made.

Missing Person Requirements:

1. A missing person over the age of 21 may be entered into the Missing Person file provided the entering agency has signed documentation supporting the conditions in which the person was declared missing. (See Missing Person Certification document from Appendix D)
    a. or when documentation from an authoritative source (a parent, legal guardian, next of kin, physician, neighbor, co-worker, etc.) is not attainable, a signed report by the investigating officer will suffice.

2. A missing person under the age of 21 must be entered within 2 hours of receipt. (A missing person report filed with an agency is sufficient documentation.)

3. The case file must contain any supporting documentation from the TIME System or other sources of information that were included in the entry. Every field must be accounted for. Below are some examples of supporting documentation.
    a. An alias name was located on a person's out of state driver's license. A copy of out-of- state driver's license file that contains the information must be included in the case file.
    b. The agency obtained dental characteristics from the individual's dentist. (Please refer to the NCIC Missing Person Dental Report in Appendix D.) The dental report and any other information that provided information within the entry must be added to the case file.
    c. The agency finds physical descriptors for an individual on their DNR file. The agency must print out the DNR response and include it in the case file.

4. The case file must contain documentation of any supplemental information added to the entry or modifications made.

Protection Order / Injunction Requirements:

1. A copy of the temporary restraining order or injunction from the clerk of circuit court must be sent to entering agency within one business day of issuance and entered by 24 hours of receipt.

a. This includes information indicating the effective period of the restraining order/injunction.
b. This includes information necessary to identify the respondent and petitioner.

2. The case file must contain any supporting documentation from the TIME System or other sources of information that were included in the entry. Every field must be accounted for. Below are some examples of supporting documentation.
    a. Alias social security number was found for the respondent on their III. A copy of the III must be included in the case file.
    b. The DOC response had additional tattoos. A copy of that printout is required.
    c. The petitioner had a legal name change and had to be added as a secondary petitioner. The printout of their DL that shows the name change should be included.

Identity Theft File Requirements*:* (The entry must be supported by an official complaint recorded by a law enforcement agency.)

1. Documentation for the complaint must meet the following criteria:
    a. Someone is using a means of identification of the victim (denoted in the Identity Theft and Assumption Deterrence Act of 1998 as any name or number that may be used alone or in conjunction with any other information to identify a specific individual.)
    b. The identity of the victim is being used without the victim's permission.
    c. The victim's identify is being used or intended to be used to commit an unlawful act.
    d. The victim has signed a consent waiver prior to entry. (Refer to the Identity Theft Consent form in Appendix D).

2. The case file must contain any supporting documentation from the TIME System or other sources of information that were included in the entry. Every field must be accounted for.

Violent Person File Requirements:

1. The agency must have documentation of one of the following criteria prior to entry:
    a. Offender has been convicted for assault or murder/homicide of a law enforcement officer, fleeing, resisting arrest, or any such statute which involves violence against law enforcement.
    b. Offender has been convicted of a violent offense against a person to include homicide and attempted homicide.
    c. Offender has been convicted of a violent offense against a person where a firearm or weapon was used.

d. A law enforcement agency, based on its official investigatory duties, reasonably believes that the individual has seriously expressed his or her intent to commit an act of unlawful violence against a member of the law enforcement or criminal justice community.

2. The case file must contain any supporting documentation from the TIME System or other sources of information that were included in the entry. Every field must be accounted for.

Gang Organization Requirements:

1. Prior to making a group entry, a law enforcement agency must complete a Group Registration Form and submit the form to CIB, who forwards the document to NCIC. NCIC will then assign a group code, which is necessary for entry. (Refer to the Gang File Group Code Request in Appendix D.) Below are the criteria for an organization to be entered and must meet the following definition:
    a. Must be an ongoing organization, association, or group of three or more persons and
    b. Must have a common interest and/or activity characterized by the commission of or involvement in a pattern of criminal activity or delinquent conduct.

***Gang Member Entry Criteria*:** (Individuals must meet two of the entry criteria excluding criteria A and I which standalone.)

A. Self-admitted gang membership at time of arrest or incarceration.
B. Identified as a gang member by a reliable informant or individual.
C. Corroborated identification as a gang member by an informant or individual of unknown reliability.
D. Frequents a documented gang's area, associated with known gang members for offenses consistent with gang activity.
E. Has been arrested on one or more occasion with known gang members for offenses consistent with gang activity.
F. Self-admitted gang membership (at any time other than arrest or incarceration
I. Has been identified as a gang member by an authorized penal organization.

2. The case file must contain any supporting documentation from the TIME System or other sources of information that were included in the entry. Every field must be accounted for.

Property Files (Vehicles, Articles, Boats, Guns, Securities, etc.) Requirements:

1. A hardcopy or electronic theft report has to have been made.

2. The case file must contain any supporting documentation from the TIME System or other sources of information that were included in the entry. Every field must be accounted for. Below are some examples of supporting documentation.
    a. DNR response with registration on a snowmobile.
    b. VIN Check response with details on the VIN of a trailer (form 0405 in Portal).
    c. Image of a boat provided by the owner.
    d. Copy of Vehicle Title.

Validation documentation requirements:

When an entry is validated, can the agency keep only the most recent version of the queries and updates made to the entry?

- Agencies can use the most recent query of the entry in the case file. However, if there is information that appears on an older version of the record, which is not present in the most recent query, those documents should be retained, or the record should be modified to remove that information.
- With regards to modifications and supplements added to the entry, the agency should show all those changes along the way and retain printouts of the modifications and supplements.

Documentation after cancellation requirements:

When an entry in the TIME System has been cancelled, how long should my agency keep the paperwork? (Example: Individual was served a warrant, hit confirmation complete and the warrant has been cancelled).

- It is CIB's recommendation that the agency hold onto the paperwork for a minimum of 18 months or until the case has concluded. However, agencies should follow their own retention policies when applicable.