TIME Agency Coordinator (TAC) Responsibilities

Each local agency accessing the TIME Systems is required to designate a TIME Agency Coordinator (TAC). Each agency having TIME System access must designate an individual employed by the criminal justice agency as the TAC. Any exceptions must be coordinated with and approved by CIB. The TAC will act as the primary liaison between their agency and the Crime Information Bureau (CIB), regularly communicating with CIB, participating in sponsored meetings, and providing feedback and recommendations for system improvement. The TAC is normally TIME System certified. The TAC will ensure that all physical, personnel, computer and communications safeguards, and security are functioning properly and are in compliance with the Department of Justice (DOJ), Crime Information Bureau, National Crime Information Center (NCIC), International Justice and Public Safety Information Sharing Network (Nlets) and International Criminal Police Association (INTERPOL) rules and regulations. Following is a list of TAC responsibilities.

A) Ensure your agency meets all applicable provisions of CJIS Security Policy, including, but not limited to the following:

1) Thorough background screening by the employing agency of personnel is required. State and national criminal history checks by fingerprint identification must be conducted **prior to granting unescorted access to Criminal Justice Information (CJI)** for all personnel who have authorized access to the TIME System and those who have direct responsibility to configure and maintain computer systems and networks with direct access to the TIME System and those with unescorted access to the secure location. The minimum check must include submission of completed applicant fingerprint cards to the FBI CJIS Division and CIB through the state identification bureau. Results must be checked on the agency's WORCS account. CIB and NCIC Wanted Person Files must also be checked. If the subject is an out of state resident, a check of the criminal history files of that state via Nlets is required. Background re-investigations are recommended every five years as good business practice. Prospective personnel must be given a copy of the Privacy Statement and Challenge Notice when fingerprinted to ensure they know they have a right to challenge the fingerprint record.

2) All personnel that configure and maintain systems and networks with access to the TIME System and those with access to criminal justice information must complete Security Awareness Training before being granted access to criminal justice information.

3) The agency must keep a current list of personnel with authorized physical or logical access. This list must be reviewed or updated annually.

4) Users may use the terminal only for those purposes for which they are authorized. The TIME System and CIB/NCIC information is only to be used by authorized law enforcement and criminal justice personnel for law enforcement or criminal justice purposes.

5) Each criminal justice agency authorized to access the TIME Systems must have a written policy for discipline of policy violators. Individuals and agencies are subject to system sanctions for policy violations. Misuse of the TIME System or information obtained from it may be a violation of state or federal laws, and individuals and agencies may be subject to criminal and/or other penalties.

6) The computer site and/or terminal areas must have adequate physical security to protect against any unauthorized personnel gaining access to the computer equipment, display, or to any criminal justice data. Agencies must control physical access to devices that display criminal justice information and shall position information system devices in such a way as to prevent unauthorized individuals from accessing and viewing criminal justice information. Agencies must control all physical access points (except for those areas within the permanent facility officially designated as publicly accessible). Utilizing publicly accessible computers to access, process, store or transmit criminal justice information is prohibited.

7) Agencies must control physical access by authenticating visitors before authorizing escorted access to the physically secure location. Retain a log of visitors accessing the secure area and review the log quarterly. The agency shall escort visitors at all times and monitor visitor activity.

8) Agencies must have access control policy and procedures. The policy and procedures must be reviewed or updated annually and after a security incident results in unauthorized access to criminal justice information or access to systems used to store, process, or transmit criminal justice information, or when changes to the CJIS security policy are made. Agencies must designate an individual with information security responsibilities to manage the development, documentation, and dissemination of the incident response policy. Use of personally owned devices to access criminal justice information is prohibited. Reference CJIS security policy Access Control section for policy requirements.

9) Agencies must have Identification and Authentication policies and procedures. The policy and procedures must be reviewed or updated annually and after a security incident results in unauthorized access to criminal justice information or access to systems used to store, process, or transmit criminal justice information. Agencies must designate an individual with information security responsibilities to manage the development, documentation, and dissemination of the incident response policy. **Agencies must deploy multi-factor authentication for all systems that transmit, process, or store criminal justice information**. Agencies must perform identity proofing procedures. Reference CJIS security policy section (IA) Identification and Authentication for policy requirements.

10) All individuals who store, process and/or transmit information on the TIME System must be uniquely identified. A unique identification shall also be required for all persons who administer and maintain the system(s) that access criminal justice information or networks leveraged for criminal justice information transit. The unique identification can be in the form of a name, badge number, serial number or other unique alphanumeric identifier. A user must uniquely identify themself before being allowed to perform any actions on the system. Agencies shall ensure that all user IDs belong to current authorized users. Identification data shall be kept current by adding new users and disabling and/or removing former users. The Crime Information Bureau must be notified in a timely manner when an individual's TIME System access should be deactivated (including, but not limited to, duty changes that no longer require TIME System access and those who are no longer employed by the agency).

11) The system shall enforce a limit of no more than five (5) consecutive invalid access attempts by a user attempting to access criminal justice information or systems with access to criminal justice information during a 15-minute period. The user account or node will automatically be locked until released by an administrator when the maximum number of unsuccessful attempts is exceeded.

12) The information system shall initiate a session lock after a maximum of 30 minutes of inactivity, and the session lock remains in effect until the user re-establishes access using appropriate identification and authentication procedures. In the interest of officer safety, devices that are part of a police vehicle or used to perform dispatch functions and located within a physically secure location, are exempt from this requirement.

13) Passwords or PINs used to access criminal justice information systems must have secure password attributes. Passwords must meet the memorized secret authenticator standards. (Reference CJIS Security Policy section IA-5(1) (a).

14) Agencies must have media protection policies that are reviewed or updated at least once a year and following any security incidents that occur at the agency. Agencies must designate an individual with security responsibilities to manage the development, documentation, and dissemination of the media protection policies and procedures. Access to CJI is restricted to authorized individuals. Criminal justice information obtained from the TIME Systems, whether electronic or physical, must be securely stored. During transport outside of secure areas, the agency shall protect and control physical media and restrict the transport of such media to authorized personnel. Agencies must document activities associated with the transport of CJI. Offsite storage of criminal justice information obtained from the TIME Systems must meet CJIS Security Policy requirements. Agencies shall restrict the use of digital and non-digital media on agency owned systems by using technical, physical, or administrative controls. Personally owned devices and digital media devices with no identifiable owner are prohibited on all agency owned or controlled systems that access, process, store, or transmit CJI.

15) Physical media must be securely disposed of when no longer needed. Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information compromise by unauthorized individuals. Physical media shall be destroyed by crosscut shredding or incineration. Electronic media storing TIME information (hard drives, flash drives, CD's, etc.) must be sanitized or degaussed using approved sanitizing software that ensures a minimal 3-pass wipe. Inoperable electronic media should be destroyed (cut up, smashed, shredded, etc.). Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel.

16) Ensure agency personnel follow rules for dissemination of criminal justice information obtained from the TIME Systems. Each data service has its own rules for secondary dissemination of records, which may include requirements for logging, identification of the purpose of the request, and identification of the specific individual receiving the record. Most records may be legitimately disseminated to another criminal justice employee or agency when the purpose of the request is criminal justice related.

    Criminal justice information (CJI) obtained from the TIME Systems may not be included in internet email transmissions unless the email is encrypted to the FIPS 140-3 standard. When email contains sensitive information, it should be standard practice to label those items as well. Fax transmission of criminal justice information is acceptable with certain encryption specifications. Fax transmission of criminal justice information over a standard phone line is exempt from encryption. If a facsimile server, application, or service which implements email-like technology to send CJI to an external physically secure location, encryption requirements for CJI in transit must be met. Voice transmission of criminal justice information (via police radio, cellular phone, etc.) is exempt from the encryption and authentication requirements when an officer determines there is an immediate need for the information in a situation affecting the safety of the officer or the general public, or the information is needed immediately to further an investigation. Any secondary dissemination of this information must meet state and federal statutes and/or regulations. Disclosure of an existing TIME System response contained within a file of the criminal justice agency, when that file is subject to a public records request, must comply with disclosure restrictions for data sources, the Wisconsin Public Records Law, and other applicable law. Note: After September 21, 2026, only FIPS 140-3 compliant encryption will be accepted.

17) The correct FBI authorized Originating Agency Identifier (ORI) shall be used in each transaction to identify the agency and/or user making the request to ensure the proper level of access for each transaction.

18) Agencies must monitor access (physical or logical) to the information system to detect and respond to security incidents and use automated mechanisms to make security alerts and advisory information available throughout the agency as appropriate.

    Agencies must have incident response policy and procedures. The policy and procedures must be reviewed or updated annually and after a security incident results in unauthorized access to criminal justice information or access to systems used to store, process, or transmit criminal justice information, security incidents that occur at the agency, or when changes to the CJIS security policy are made. Agencies must designate an individual with information security responsibilities to manage the development, documentation, and dissemination of the incident response policy. Agencies shall provide incident response/ breach training on how to identify and respond to a security incident. Personnel should know how to report a security incident, who to report an incident to, when to contact that person, and what basic actions to take in case of a suspected compromise of the system. This may include contacting a supervisor, contacting on-call information technology staff, disconnecting the affected computer from the network, etc. Agency staff should document any security incidents including possible or attempted security incidents and promptly report incident information to the Crime Information Bureau. Evidence of the security incident may need to be collected and retained to conform to the rules of evidence in case of legal action (either civil or criminal).

19) Agencies must have System and Information Integrity policies and procedures. The policy and procedures must be reviewed or updated annually and after a security incident results in unauthorized access to criminal justice information or access to systems used to store, process, or transmit criminal justice information. Agencies must designate an individual with information integrity responsibilities to manage the development, documentation, and dissemination of the incident response policy.

20) Agencies connecting to the TIME Systems are required to monitor the system to detect intrusion and anomalous activities by deploying malicious code protection, virus protection, spam and spyware protection in place at critical points throughout the networks and on all workstations, servers, and mobile

computing devices on the network. Malicious code protection must be enabled and must include automatic updates for all systems with Internet access. Agencies with systems not connected to the Internet must implement local procedures to ensure malicious code protection is kept current (i.e., most recent definitions update available). Resident scanning must be employed. Agencies must monitor applications, services, and information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws. System patches shall be installed in a timely manner.

21) Agencies using electronic handheld devices, mobile devices and/or laptops to access TIME information must implement the security requirements as outlined in the CJIS Security Policy. This may include multi-factor authentication, encryption, security-related updates, official use guidance, data at rest encryption, and prevention of data compromise in case of possible loss of the device. A personal firewall must be employed on all devices that are mobile by design (i.e., laptops, handhelds, personal digital assistants, etc.).

22) Criminal justice information that is at rest or stored electronically outside the boundary of the physically secure location shall be Federal Information Processing Standard (FIPS) 140-3 compliant. Data transmitted outside the boundary of the physically secure location shall be encrypted to the FIPS 140-3 standard. Criminal justice data passing through a telecommunication infrastructure that is shared by criminal justice and non-criminal justice users must be encrypted to the FIPS 140-3 standard. Note: After September 21, 2026, only FIPS 140-3 compliant encryption will be acceptable.

23) Ensure the criminal justice agency has a Local Agency Security Officer (LASO) assigned. The LASO is responsible for: identifying who is using the agency's approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access. Identifying and documenting how the equipment is connected to the state system. Ensuring that personnel security screening procedures are being followed and the approved and appropriate security measures are in place and working as expected. The LASO supports policy compliance and ensures the CIB is promptly informed of security incidents. Ensure the LASO completes the required annual training.

24) Agencies must have system maintenance policy and procedures. The policy and procedures must be reviewed or updated annually and after a security incident results in unauthorized access to criminal justice information or access to systems used to store, process, or transmit criminal justice information. Agencies must designate an individual with security responsibilities to manage the development, documentation, and dissemination of the system maintenance policy. Agencies must maintain maintenance records, use approved tools for non-local maintenance which meet multifactor authentication and encryption requirements, and prevent unauthorized removal of maintenance equipment.

25) Agencies must replace system components when support for the component(s) is no longer available from the original manufacturer, or original contracted vendors.

26) Agencies must have awareness and training policies. The awareness and training policy must be reviewed or updated at least once a year and following changes to information system operating system, when security incidents that occur at the agency, or when changes to the CJIS security policy are made. Agencies must designate an individual with information security responsibilities to manage the development, documentation, and dissemination of the awareness and training policies and procedures. The policy must be disseminated to all users who have unescorted logical or physical access to an information system that provides access to unencrypted criminal justice information.

27) Agencies must employ one or more of the following techniques to increase 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, or conducting awareness events.

28) Agencies must regularly scan their system and applications for vulnerabilities (e.g. out-of-date software, poorly configured network device). Utilize tools that can help automate and coordinate vulnerability scanning, remediation and help measure the impact of vulnerabilities. Review the results of vulnerability scans and share them with organizational personnel with risk assessment to ensure similar vulnerabilities are remediated within the prescribed timelines. Vulnerability scanning tools must

be kept up to date to ensure they can detect new vulnerabilities.

29) Agencies must document their system/network baseline configuration, system inventory and represent their network with a network diagram. Review and update the network diagram, baseline configuration and network inventory yearly, when changes are made or after a security incident. At least one previous version of the configuration is required to support a system rollback. The baseline configurations are to be updated when configuration changes are made.

30) Document and establish secure configurations for system components, ensure configuration provides only essential capabilities using established best practice guidelines and prohibit non-essential services, software etc. from running. Utilize automated processes to detect unauthorized hardware, components, software etc.

B) Ensure that the agency's Acadis roster is updated in a timely manner.

C) Ensure that new employees review the TIME System New Operator Handout.

D) Ensure within six months of employment or assignment that all personnel accessing TIME/NCIC have completed the required TIME System training. This includes *e*TIME, MDT/MDC, Basic or Advanced certification. Security Awareness and LASO training must be completed **prior to assignment of a position**.

E) Ensure that all personnel accessing criminal justice information complete recertification biennially (every two years). Ensure all personnel complete Security awareness training annually. Ensure personnel assigned with security responsibilities complete LASO training annually.

F) Maintain records of all personnel's TIME System training and testing.

G) Ensure all computer terminals are updated with the most current version of TIME System software.

H) Ensure that the Portal XL access (initial access as well as level of access) is properly requested for agency personnel who will use this software.

I) Provide instructional material for the functional use of the local equipment, software, and formats to be used for TIME System applications.

J) Ensure TIME System Newsletters and related correspondences are disseminated and available to the appropriate personnel. This includes briefing administrative staff whenever appropriate.

K) If applicable, ensure signed agency agreements are on file with criminal justice agencies that your agency provides with TIME service or information. A Management Control Agreement (MCA) is required if a criminal justice agency contracts with a non-criminal justice governmental agency for IT support, housing/storing hardware for the criminal justice agency, or performing criminal justice functions on behalf of the criminal justice agency (dispatch, pre-trial screening, etc.). The non-criminal justice agency only has access to TIME System information because the criminal justice agency allows them to act on behalf of the criminal justice agency.

L) If applicable, ensure the agency keeps signed copies of the Security Addendum for all individuals that work for private entities / companies that have physical or network access.

M) When appropriate, ensure INTERPOL and ALPR agreements are on file.

N) Ensure the department has written policies and procedures in place as required by CIB and CJIS standards. Ensure policies and procedures are updated when necessary.

O) The TAC is responsible for providing assistance/information during CIB/NCIC audits.

P) Ensure compliance with the criminal history record inquiry requirements of CIB/NCIC, including creation of a secondary dissemination log, identifying the requesting individual, proper use of purpose codes, and justification for each inquiry.

Q) Ensure all monthly validations are completed on time and exception report records are handled per instructions.

R) The TAC should understand the record system and communications capabilities of their agency.

S) Ensure that CIB is advised of any change in the status of the TAC by emailing cibtrain@wisdoj.gov. Change in TAC status may be due to reassignment, promotions, etc. Prior to leaving an agency, current TAC is to choose a replacement TAC and notify CIB in a timely manner to allow for a smooth transition.