TIME Agency Coordinator (TAC) Responsibilities

Each local agency accessing the TIME/NCIC 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.

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

   A) 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. 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.

   B) All personnel that configure and maintain systems and networks with access to the TIME System and those with access to criminal justice information have completed the required Security Awareness Training.

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

   D) 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.

   E) Each criminal justice agency authorized to access the TIME/NCIC 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.

   F) 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.

G) Agencies must control physical access by authenticating visitors before authorizing escorted access to the physically secure location. The agency shall escort visitors at all times and monitor visitor activity.

H) 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 currently authorized users. Identification data shall be kept current by adding new users and disabling and/or deleting 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).

I) 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. If a user is unable to successfully gain access to the system within five (5) attempts, the users account will automatically be locked for at least a 10-minute period unless released by an administrator.

J) 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 reestablishes 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.

K) Passwords used to access criminal justice information systems must have secure password attributes. Passwords must meet either the Basic Password standards or the Advanced Password standards.

- Basic Passwords standards: must be a minimum length of 8 characters; must not be a dictionary word or proper name; and cannot be the same as the user ID; must expire within a maximum of every 90 calendar days; cannot be identical to the previous ten passwords; cannot be displayed on screen when entered; and must not be transmitted in the clear outside the secure location.
- Advanced Password standards: passwords shall be a minimum of twenty (20) characters in length with no additional complexity requirements imposed; password verifiers shall not permit the use of a stored "hint" for forgotten passwords and/or prompt subscribers to use specific types of information when choosing a password; verifiers shall maintain a list of "banned passwords" that contains values known to be commonly-used, expected, or compromised; verifiers shall compare the prospective passwords against the "banned passwords" list; reject prospective passwords which are part of the banned password list; verifiers shall force a password change if there is evidence of authenticator compromise or every 365 days from the last password change; verifiers shall use approved encryption and an authenticated protected channel when requesting passwords to protect against eavesdropping and Man-in-the-Middle (MitM) attacks; verifiers shall store passwords in a manner that is resistant to offline attacks by salting and hashing the password using a one-way key derivation function when stored; and verifiers shall protect stored salt and resulting hash values using a password or PIN.

L) Criminal justice information obtained from the TIME/NCIC 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. Offsite storage of criminal justice information obtained from the TIME/NCIC Systems must meet CJIS Security Policy requirements.

M) 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 shredding, incineration, etc. Electronic media storing TIME/NCIC 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.

N) Ensure agency personnel follow rules for dissemination of criminal justice information obtained from the TIME/NCIC 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/NCIC Systems may not be included in an internet email transmission unless the email is encrypted to the FIPS 140-2 certified 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.

O) 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.

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

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).

Q) Agencies connecting to the TIME/NCIC Systems are required to have malicious code protection, virus protection, spam protection 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.

R) Agencies using electronic handheld devices, mobile devices and/or laptops to access TIME/NCIC information must implement the security requirements for such access as outlined in the CJIS Security Policy. This may include advanced 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. The requirement to use or not use advanced authentication is dependent upon the physical, personnel and technical security controls associated with the user location as specified in the CJIS Security Policy. A personal firewall must be employed on all devices that are mobile by design (i.e. laptops, handhelds, personal digital assistants, etc.).

Ensure that personally owned equipment used to access the TIME/NCIC Systems or used to access data obtained from those systems meets all applicable requirements set forth in the CJIS Security Policy.

S) Criminal justice information that is at rest or stored electronically outside the boundary of the physically secure location must be encrypted to FIPS 140-2 standard. Data transmitted outside the boundary of the physically secure location must be encrypted to the FIPS 140-2 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 140-2 standard.

T) 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; ensuring the approved and appropriate security measures are in place and working as expected; and support policy compliance and ensure the CIB is promptly informed of security incidents. Ensure the LASO completes the required annual training.

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

3) Ensure within six months of employment or assignment that all personnel accessing TIME/NCIC have completed the required TIME System training. This includes Security Awareness, *e*TIME, MDT/MDC, Basic or Advanced certification.

4) Ensure that advanced project results are reviewed with the employee when received.

5) Ensure that all certified operators, no matter the certification level, are provided with the opportunity to take annual in-service training (online module or paper copy).

6) Ensure all personnel accessing criminal justice information complete recertification biennially.

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

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

9) Ensure that the Portal 100 access is properly requested for agency personnel who will use this software.

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

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

12) Ensure signed agency agreements are on file with criminal justice agencies that your agency provides with TIME service or information.

13) When appropriate, ensure signed management control, INTERPOL and ALPR agreements are on file.

14) 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.

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

16) 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.

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

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

19) Ensure that CIB is advised of any change in the status of the TAC due to reassignment, promotions, etc.