WISCONSIN

TIME SYSTEM

Training Materials

TIME SYSTEM SECURITY AWARENESS HANDOUT

Revised: 12/14/2021
2022 Security Awareness Handout All

System Security

The TIME/NCIC Systems are criminal justice computer networks that provide access to sensitive and sometimes confidential information, such as driver's license records, criminal history records, wanted person records, etc. This information must be protected from those who would try to gain unauthorized access to the system and those who would use information obtained from the system for unauthorized purposes.

Various agencies have agreed to make their information available to law enforcement and criminal justice agencies via the TIME and NCIC Systems for the specific purpose of facilitating the administration of criminal justice. Any misuse of this information or violation of the understandings and policies of the system jeopardizes the availability of information for all participating agencies.

The FBI's CJIS Security Policy establishes *minimum* information security requirements to protect information sources, transmission, storage, and creation of criminal justice information. The TIME System has adopted the CJIS Security Policy as the TIME System Security Policy. Each agency and user accessing the system is responsible for ensuring the security of the system and criminal justice information.

Authorized Personnel

TIME/NCIC System information is only to be used by *authorized* law enforcement/criminal justice personnel for law enforcement/criminal justice purposes as outlined in the CJIS Security Policy Section 5.12. Authorized personnel are those that have undergone the required fingerprint-based background check, completed security awareness training and appear on the agency's list of authorized personnel.

System Usage

TIME/NCIC System information is ***only*** to be used by authorized law enforcement/criminal justice personnel for law enforcement/criminal justice purposes. Both conditions must be met. For example, a law enforcement officer may not obtain license plate/vehicle registration information for personal reasons.

Each criminal justice agency authorized to access the TIME/NCIC Systems is required to have a written policy for discipline of policy violators. Misuse of the TIME System or information obtained from it may be a violation of state or federal laws, and violations may subject individuals and agencies to criminal prosecution and/or other penalties. The unauthorized request, receipt, or release of TIME/NCIC System information can and *has* resulted in criminal/civil proceedings.

Physical Access & Visitors

Agencies must control all entrances to the secure area and must verify that an individual qualifies for access before granting admission. Remember, authorized personnel are those that have undergone the required fingerprint-based background check, completed security awareness training and appear on the agency's list of authorized personnel. If a person has not met these requirements, they may only access the secure area if they are escorted by someone who is authorized.

Before granting such a visitor escorted access to the secure location you should verify the visitor's identity. Visitors must be escorted at all times and visitor activity must be monitored.

Personnel should be aware of their surroundings and take steps to ensure unauthorized persons do not access criminal justice information or the TIME/NCIC Systems. This may include challenging or questioning unescorted subjects, verifying credentials of strangers, and/or ensuring visitors and other unauthorized users are not looking over someone's shoulder to get information. Numerous techniques and tools exist to help ensure the security of data. These may include the use of screensavers, screen shields, terminal location and positioning, etc.

Agency personnel should ensure that all people abide by entrance and exit procedures, visitor control, handling procedures, and access control points. Personnel should report violations or suspected violations, including areas that may not be secure.

Using publicly accessible computers to access, process, store or transmit criminal justice information is prohibited. Publicly accessible computers include, but are not limited to hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.

Logins

A unique login ID is required for each individual who is authorized to store, process, and/or transmit criminal justice information. This includes all persons who administer and maintain the system/network that accesses and/or transmits TIME/NCIC information. Users are required to uniquely identify themselves before they are allowed to perform any actions on the system.

By logging into and accessing the system and the information contained therein, users are signifying their agreement to abide by all system policies and procedures and acknowledging the possible consequences of misuse of system resources or criminal justice information. *Users should protect their logins and not share them with anyone.* Users are responsible for any and all system activity that happens under their login.

If a user is unable to log in after five (5) consecutive invalid access attempts, their account will be automatically locked for at least ten (10) minutes unless released by an administrator. In addition, the system will initiate a session lock after a maximum of thirty (30) minutes of inactivity. The session lock will remain in effect until the user once again establishes access using appropriate login and authentication. In the interest of officer safety, devices that are part of a criminal justice conveyance, used to perform dispatch functions or designated solely for the purpose of receiving alert notifications and are staffed when in operation and located within a physically secure location are exempt from this requirement.

Passwords

Passwords used to access the TIME/NCIC Systems must meet specific standards to be secure passwords as presented in 5.6.2.1.1 (Basic Password Standards) or 5.6.2.1.2 (Advanced Password Standards) of the CJIS Security Policy.

Basic Passwords Standards: Passwords must be at least eight (8) characters, must not be a dictionary word or proper name, and cannot be the same as the user ID. Passwords must expire at least every 90 calendar days and cannot be identical to the previous ten passwords used. Passwords cannot be displayed on screen when entered and must not be transmitted in the clear outside the secure location. *Users should protect their passwords and not share them with anyone.*

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 and 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. Verifiers shall protect stored salt and resulting hash values using a password or PIN.

System users should be aware of subjects attempting to obtain computer system access or password/login information by using 'social engineering'. Social engineering means manipulating people into doing something or divulging confidential information. This may include emails from unknown sources, email attachments containing spyware programs, telephone callers purporting to be from another authorized agency, etc. When in doubt, system users should verify the source or identity behind the email, telephone call, etc. before potentially misusing system resources or providing criminal justice information to unauthorized subjects.

Proper Handling of Criminal Justice Information

Information obtained via the TIME/NCIC systems, whether in paper form or saved digitally, must be stored in a secure area inaccessible to the public.

Criminal justice information obtained from the TIME/NCIC Systems should remain in the secure area unless there is specific authorization and procedures for taking the information out of the secure area. When TIME/NCIC information (paper or digital) is transported outside of the secure areas it must continue to be protected, thus transport of TIME/NCIC information is restricted to authorized personnel.

TIME/NCIC information must be securely disposed of when no longer needed. Destruction of paper information may be accomplished by shredding, incineration, etc. Digital 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 digital media should be destroyed (cut up, smashed, shredded, etc.). The disposal or destruction of TIME/NCIC information must be witnessed or carried out by authorized personnel to avoid the possibility of inadvertent release of system information to unauthorized persons.

Dissemination of Criminal Justice Information

Any individual authorized to use the TIME/NCIC System who receives a request for system information from another individual must ensure the person requesting the information is authorized to receive the data. The correct Originating Agency Identifier (ORI) must be used in each transaction to identify the agency receiving the information to ensure the proper level of access for each transaction.

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/agency when the purpose of the request is criminal justice related.

Any secondary dissemination of this information must meet state and federal statutes and/or regulations.

Criminal justice information 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 standard. When email contains sensitive information, it should be standard practice to label those items as well.

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.

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 (CJIS Security Policy Section 5.10).

Criminal Justice Information that is introduced into the court system pursuant to a judicial proceeding and that can be released to the public via a public records request is not subject to the CJIS Security Policy.

Security Incidents & Response

A security incident is a violation or possible violation of policy that threatens the confidentiality, integrity or availability of criminal justice information. There has been an increase in the number of accidental or malicious computer attacks against both government and private agencies, regardless of whether the systems are high or low profile.

Indicators of a security incident may include system crashes without a clear reason, new files with novel or strange names appearing, changes in file lengths or modification dates, unexplained poor system performance, etc.

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/possible 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).

Agencies must monitor physical access to the information system to detect and respond to physical security incidents, and wherever feasible the agency shall employ automated mechanisms to make security alert and advisory information available throughout the agency as appropriate.

Virus/Spam/Spyware & Malicious Code Protection

To ensure information security, agencies connecting to the TIME/NCIC Systems are required to have in place malicious code protection, virus protection, spam protection and spyware protection. Users should be cautious when downloading internet content or clicking on web-based pop-ups/windows, unknown emails, email attachments or embedded objects. Removable devices such as flash drives, CDs, etc. may also possibly introduce viruses/malware and caution should be used before they are introduced to the system. Follow your agency's policies regarding use of such items.

Technical Considerations

Mobile Devices – Handheld Devices, Laptops, etc.

As digital handheld devices continue to become more integrated into the mobile workforce, security measures must be employed since such devices may be used outside of physically secure locations. Wireless devices, even in physically secure areas, are susceptible to penetration, eavesdropping and malware. Furthermore, compromised or lost wireless devices may introduce risk to the overall security of an agency's network, criminal justice information and/or the TIME/NCIC Systems. The use of digital handheld devices and/or laptops to access TIME/NCIC information is allowed, provided the agency implements the security requirements for such access as outlined in the CJIS Security Policy. This may include mobile device management, 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.

Personally-owned information systems shall not be authorized to access, process, store or transmit criminal justice information unless the employing agency has established and documented policies and procedures for such use. All devices must be authorized and must meet the requirements set forth by 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.).

Mobile devices used to access the TIME/NCIC Systems may be agency-owned or personally-owned. Personally-owned equipment used to access the TIME/NCIC Systems or used to access data obtained from those systems must meet all the requirements set forth in the CJIS Security Policy. Agencies wishing to use personally owned devices for system access must first document the specific terms and conditions for such use. Such documentation should consider licensing issues, agency control, security requirements, and sanitization of the device if the owner no longer carries out law enforcement duties, etc.

Account Management

User logins/accounts should be kept current, when a user is terminated, leaves employment or job duties no longer require TIME/NCIC System access the user's system account should be disabled. An agency must validate system accounts at least annually.

User TIME/NCIC accounts will be assigned according to the principle of 'least privilege'. Least privilege means giving a user account only those privileges which are essential to perform assigned duties. Assigned authorizations will control access to the system and system information.

Users may only have one active computer session accessing the TIME/NCIC Systems at a time. Multiple concurrent active sessions for one user are prohibited unless the agency can document a business need for such multiple session access.

System Updates

Malicious code protection, virus protection, spam protection and spyware protection must be 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.

Backup & Storage Procedures

Agencies must consider the requirements for secure storage of digital media and hardware containing criminal justice information, and ensure that such backup procedures, archiving, and storage, whether centralized or de-centralized (off site) meet the security requirements outlined in the CJIS Security Policy.

TIME System Security Awareness
Certification Statement

I certify that I have read and understand the contents of the TIME System Security Awareness handout and agree to follow all TIME/CJIS Systems requirements regarding the proper access to, use of, storage, and disposal of TIME/CJIS System information.

I understand that the criminal justice information made available via the TIME/CJIS Systems is sensitive and has potential for great harm if misused; therefore, access to this information is limited to authorized personnel. I understand that misuse of the TIME/CJIS systems or information received from these systems may subject me to system sanctions/penalties and may also be a violation of state or federal laws, subjecting me to criminal and/or other penalties. Misuse of the TIME/CJIS Systems includes accessing the systems without authorization or exceeding my authorized access level, accessing the systems for an improper purpose, using or disseminating information received from the systems for a non-work related or non-criminal justice purpose, etc.

Your signature:_____

Print your name:_____

Agency name:_____

Date:_____