



WISCONSIN TIME SYSTEM

Training Materials

TIME SYSTEM SECURITY AWARENESS HANDOUT

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 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.

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 criminal justice professional 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.

Proper Handling of Criminal Justice Information

Information obtained via the TIME/NCIC systems, whether in physical or digital format, must be stored in a secure area accessible only to authorized personnel. Agencies must mark system media indicating distribution limitations, handling caveats, and applicable security markings of the information. Physical and digital media which remain within the physically secure location are exempt from media marking requirements.

Criminal justice information obtained from the TIME/NCIC Systems should remain in the secure area unless there is specific authorization and procedures for removing information

from the secure area. Agencies must physically control and securely store digital and non-digital media within physically secure locations or controlled areas and encrypt CJI on digital media when physical and personnel restrictions are not feasible. Agencies must protect system media until the media is destroyed or sanitized.

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. Agencies must protect and control digital and non-digital media to prevent compromise of the data during transport outside of the physically secure locations or controlled areas. Digital media shall be protected by using encryption. Physical media must be protected at the same level as the information would be protected in electronic form. Agencies must maintain accountability for system media during transport outside of the physically secure location or controlled areas as well as document activities associated with the transport of system media and restrict the activities associated with the transport of system media to authorized personnel.

Physical media will be securely disposed of when no longer needed for investigative or security purposes, whichever is later. Physical media will be destroyed by crosscut shredding or incineration and agencies must employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information. 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 minimum 3-pass wipe. Inoperable digital media should be destroyed (cut up, smashed, shredded, etc.). The sanitization, disposal, and 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.

Agencies must restrict the use of digital and non-digital media on agency owned systems that have been approved for use in the storage, processing, or transmission of criminal justice information by using technical, physical, or administrative controls. Agencies must prohibit the use of personally owned digital media devices on all agency owned or controlled systems that store, process, or transmit CJI. Agencies must 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.

Agencies must have policies and procedures related to media protection including an agency-level media policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance and is consistent with applicable laws and regulations. All agency personnel must be aware of the media protection policies and procedures. Agencies must review and update these policies and procedures at least once a year and following any security incidents involving digital or non-digital media. Agencies must designate an individual with security responsibilities to manage the development, documentation, and dissemination of the media protection policy.

Access

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.

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.

System users should be aware of subjects attempting to obtain access to confidential information via "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.

Incident Response

A security incident is a violation or possible violation of policy that threatens the confidentiality, integrity or availability of TIME/NCIC information.

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 TIME/NCIC Systems or criminal justice information obtained from them.

TIME System Security Awareness Certification Statement

I certify that I have read and understand the contents of the TIME System Security Awareness Physical Access 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: _____