TIME and CJIS Systems Use and Dissemination of Records

Eff. Date 03/16/2026

Purpose

The Madison Police Department (MPD) uses the Transaction Information for the Management of Enforcement (TIME) System/eTIME (online version of TIME) and additional CJIS systems to access privileged information. TIME/eTIME grants access to the following data service agencies:

- Wisconsin Department of Justice Crime Information Bureau (CIB)
- Federal Bureau of Investigations (FBI) Criminal Justice Information Services (CJIS) Division
- FBI National Crime Information Center (NCIC)
- National Law Enforcement Telecommunication System (NLETS)
- Canadian Police Information Centre (CPIC)
- Wisconsin Department of Transportation (DOT)
- Wisconsin Department of Natural Resources (DNR)
- Wisconsin Department of Corrections (DOC)
- Additional CJIS Information Systems
- National Data Exchange (N-Dex)
- Law Enforcement Information Exchange (LInX)
- Law Enforcement Enterprise Portal (LEEP)

Procedure

SYSTEM USAGE

ONLY authorized users shall access TIME and CJIS systems for <u>valid</u> law enforcement/criminal justice purposes. At no time will any user use TIME and CJIS systems to run the user's personal information (and respective license plates), a family member's information, or information for anyone with whom the user is closely associated. Should a situation arise wherein the subject who needs to be run through TIME and CJIS systems is closely affiliated with the user, the user will request another officer, staff member, or a supervisor to run the subject. If a test record needs to be run, only approved test transactions should be used.

PENALTY FOR MISUSE

The Department of Justice Crime Information Bureau, as well as the MPD, may investigate any alleged misuse of TIME and CJIS Systems. Potential misuse of these systems includes running family members or other subjects with whom the user is closely associated for criminal justice purposes during the normal course of work, running information for personal use, and running information that is in direct conflict with the regulations set forth by the FBI and CIB for the use of the TIME system. Individuals determined to have misused the TIME system may be subject to internal discipline and/or criminal and/or civil penalties under state and federal law. TIME and CJIS system logs are routinely audited for compliance with these policies.

SECURITY

TIME Agency Coordinator

The MPD shall designate an individual to serve as a TIME Agency Coordinator (TAC). The TAC may designate authorized contacts to fulfill various roles and responsibilities in the administration of the TIME system. Responsibilities of the TAC include ensuring that authorized users are trained and in compliance with CJIS, FBI, and MPD policies and regulations. The TAC also serves as the administrator of TIME interfaces to departmental applications/systems, terminal designations, and applicable communications/connectivity. Additionally, the TAC is responsible for the completion of audits performed by CIB and the FBI. In order to

maintain our agency's access to the TIME system, it is essential that all staff comply with all requests from the TAC or designee(s). Additionally, the TAC will disseminate TIME System Newsletters to departmental staff.

General Security

Access to TIME and CJIS terminals shall be limited so that only authorized users will be able to view and access information from the system. In order to qualify for authorization upon hiring, a TIME and CJIS user must undergo identity verification and background screening. This includes:
- Providing acceptable identity documentation (driver's license, passport, I-9 completion, etc.)
- Completing a background check conducted by MPD staff
- Completing a fingerprint based criminal history check
- Complete initial certification within six months of hire

Additionally, users must continue to maintain applicable TIME and CJIS certifications bi-annually, and user. User access to TIME and CJIS systems shall be reviewed at least once per year. Users granted access to TIME and CJIS systems, shall be provided with the minimum level of permissions to meet respective job duties. Upon termination of employment, a user's account shall be disabled, access removed, and CIB contacted to update departmental records. Staff with agencies holding a current Management Control Agreement with MPD will be required to complete and maintain TIME System Security Awareness training. Vendors remotely accessing CJIS related applications/systems shall be virtually escorted by certified and authorized MPD Technology staff. In the event of a security incident, the occurrence shall be documented and reported to CIB in accordance with applicable policies and procedures.

CRIMINAL HISTORY RECORD INFORMATION (CHRI/III/CJIS)

Information from Criminal History Record Information (CHRI), the FBI Interstate Identification Index (III), and CJIS systems shall only be obtained for designated purposes outlined below. This information is not to be disseminated to non-criminal justice agencies or persons. Dissemination to another criminal justice agency requires a secondary dissemination log that will be maintained for one year. The original authorized user must ensure that the recipient is properly authorized, and for valid purposes, to receive the information. CHRI/III/CJIS records received cannot be disseminated via radio broadcast or cellular phones unless there is a situation affecting officer safety or the general public.

Authorized Purpose Codes

- **Code C:** Code C is used for Criminal Justice/Law Enforcement purposes and is accepted by CIB and by the FBI. Adult and juvenile records will be supplied. This code is used for official duties in conjunction with the administration of justice (such as detection, apprehension, detention, prosecution, etc.).
- **Code J:** Code J is used for Criminal Justice/Law Enforcement employment applicants and is accepted by CIB and by the FBI. Adult and juvenile records will be supplied.
- **Code D:** Code D is used Domestic Violence/Stalking and is accepted by CIB (only adult records will be returned) and by the FBI (only returns information not sealed by state). This code is used by agencies providing a record to a court hearing for Domestic Violence and is for court use only. Actual Domestic Violence incidents will use Code C.
- **Code H:** Code H is used for checking suitability of Public Housing Applicants and is accepted by CIB (for adult records only) and by the FBI (for identification only).
- **Code F:** Code F is used for the return of Firearms to Lawful Owner and is accepted by CIB and by the FBI. Both adult and juvenile records are supplied. This code is used for the return of firearms to owners after theft, improper seizure, etc.
- **Code E:** Code E covers other Authorized Employment Purposes and is accepted by CIB ONLY (which ONLY supplies adult records). The FBI will not accept this code. This code is used for when criminal history is required by state statute, local ordinance, or federal regulation.

Storage and Disposal of CHRI Information

CHRI/III/CJIS records shall not unnecessarily be maintained in case files to avoid disclosure of out-of-date/inaccurate records under Wisconsin open records law. Cases that are e-Referred may contain CHRI/III/CJIS information; however, this information is not considered part of the case documentation and is not subject to open records. When no longer needed, data from TIME and CJIS Systems shall be disposed of by the user in a secure manner via shredding.

Probable Cause/Hit Confirmation

A hit on TIME is not sufficient for probable cause and only comprises part of the probable cause analysis and must be viewed in conjunction with other available information. As the time period increases since the receipt of the hit, the significance of the hit decreases. When a hit confirmation request is received via dispatch or directly to the Officer in Charge (OIC), the 911 data operator, on behalf of MPD, will provide timely confirmation back to the requesting agency.

CHRI/III INFORMATION

On the CHRI/III/CJIS request screens, the attention field shall contain the user's IBM number/badge number and the additional information field shall contain the case number. If no case number exists, a brief explanation of why the request was run is required.

TIME and NCIC Management of Records

Only staff with Advanced TIME Certifications shall be allowed to enter, modify, and remove records from TIME/NCIC. Once a record has been entered or modified, a secondary check will be completed by a staff member who did not enter or modify the original record. Validation of all entries into TIME/NCIC shall be completed as designated by CIB.

Original SOP: 02/25/2015
(Reviewed Only: 02/04/2016, 02/05/2024)
(Revised: 01/06/2017, 12/11/2017, 11/18/2019, 11/29/2021, 03/04/2022, 07/12/2022, 05/19/2025, 03/16/2026)