WISCONSIN

TIME SYSTEM

Training Materials

TIME SYSTEM
NEW
OPERATOR TRAINING

Revised 12/14/2021
(2022 New Operator.doc)

TO: New TIME System Operators

FROM: The Crime Information Bureau (CIB)

RE: **TIME System - New Operator Training**

This handout will help familiarize you with the Transaction Information Management of Enforcement (TIME) System operations. Your agency's TIME Agency Coordinator (TAC) or Agency Assigned Instructor (AAI) should review this handout with you, demonstrate TIME System terminal operation and answer any questions you may have.

You must achieve TIME System Certification, at the appropriate level, within 6 months of employment or assignment as a terminal operator.

ALL TRANSACTIONS SENT ON THE TIME SYSTEM MUST DEAL WITH AUTHORIZED LAW ENFORCEMENT OR CRIMINAL JUSTICE RELATED MATTERS

DIVISION OF LAW ENFORCEMENT SERVICES (DLES)

INTRODUCTION

The Wisconsin Department of Justice (DOJ) was created in 1967 and placed under the Office of the Attorney General. The Division of Law Enforcement Services (DLES) includes the Training and Standards Bureau, the Bureau of Justice Programs, the Bureau of Justice Information and Analysis, and the Crime Information Bureau (CIB). The division aids federal, state, and local criminal justice agencies. The division provides support to law enforcement units in their efforts to detect and apprehend criminal offenders and assists them in their responsibility to control crime.

The legislation that created the Division of Law Enforcement Services also established two information systems to serve Wisconsin criminal justice agencies. These systems are a centralized fingerprint identification and criminal history record information repository, and a computerized communications system known as Transaction Information for Management of Enforcement (TIME). These systems provide an integrated information base vital to the day-to-day operations of criminal justice agencies. Criminal justice data is collected, processed, and disseminated in in a manner useful for administrative and operational tasks. The law requires certain specific types of data be contributed by law enforcement agencies, the courts, and correctional agencies/facilities to accomplish these goals and allow for efficient management of the two information systems.

Criminal History Unit

The criminal history unit is responsible for maintaining Criminal History Record Information (CHRI), including demographic information, arrest and charge information, and related final disposition reports from the District Attorney/Prosecutor, Clerk of Court, municipal court, or correctional agencies. The criminal history unit works cooperatively with submitting agencies to ensure records are accurate. Requests for expungements or challenges to criminal history information are processed by this unit.

A master set of fingerprints for each State Identification Record (SID) are maintained within the Automated Fingerprint Identification System (AFIS), a system managed and maintained by the Division of Forensic Science. As new fingerprints are received, they are compared to the master set of prints. If the new prints match an existing SID the new event information is added to that SID. If no match is found a new SID is created containing the new event information. Wisconsin is a contributor to the FBI's Interstate Identification Index (III). III is the national criminal history repository; all fingerprinted arrests events for individuals treated as an adult are automatically submitted to the III database.

The criminal history unit also provides public access to CHRI and manages the Wisconsin Online Record Check System (WORCS). Anyone may obtain this information from CIB provided they pay the fee established by the legislature. The public is prohibited from accessing juvenile information, which is restricted by law.

The unit is also responsible for the following:

- Processing all incoming and outgoing electronic or paper documents
- Scanning paper fingerprint submissions or correcting errored livescan submissions
- Corrections of electronic or paper dispositions
- Archival of correspondence and photographs submitted electronically or by paper

Firearms Unit

Wisconsin statutes require all Wisconsin firearms dealers licensed by the Federal Bureau of Alcohol, Tobacco and Firearms to request the CIB Firearms Unit to conduct a background check of any person attempting to purchase a handgun in Wisconsin. The purpose of this background check is to ensure that the person wishing to purchase the handgun is eligible to possess the handgun under state and federal laws.

State and federal laws prohibit possession of a firearm if a person has been convicted of a felony, indicted in any court for a crime punishable by imprisonment greater than one year, persons adjudicated delinquent for an act that if committed by an adult in this state would be a felony, subject to a court order or injunction restraining them from harassing, stalking or threatening an intimate partner or child of such partner, discharged from the Armed Forces under dishonorable conditions, adjudicated mentally defective, is an unlawful user of any controlled substance, is an alien unlawfully in the United States, or is a fugitive from justice. In accordance with Federal law, this includes some out-of-state misdemeanor and felony warrants.

Utilizing the Firearms Dealer Notification Form, all registered firearms dealers are required to contact the CIB Handgun Hotline to request a background check be performed on the purchaser before transferring a handgun. The firearms unit has five working days, not including weekends and holidays to complete the firearms background check. Upon completion of the background check the dealer is given an approval number or a denial number for the transfer of the handgun. The dealer may not transfer the firearm to the purchaser until they receive an approval number from CIB.

TIME and Technical Services Unit

The TIME and Technical Services Unit is responsible for a wide variety of services and systems within the department. The TIME System mentioned earlier is overseen by this unit. TIME System is a computerized communications system that became operational in 1972. The system enables federal, state, and local law enforcement agencies to access multiple Wisconsin data sources for various types of information essential to police operations (driver and vehicle information, Wisconsin criminal history information, etc.). The system also provides an automated interface with the FBI's National Crime Information Center (NCIC) operated by the Criminal Justice Information Services (CJIS) Division furnishing information of national concern, including national criminal history record information. In addition, TIME System agencies have access to the Canadian Police Information Centre (CPIC) and the International Justice and Public Safety Information Sharing Network (Nlets). The TIME System acts as a hub facilitating the exchange of information between law enforcement agencies within Wisconsin.

Every state has a control center that is responsible for operating and maintaining its law enforcement telecommunications system, such as the TIME System. Control centers operate 24 hours a day, seven days a week. The control center is responsible for monitoring transactions being sent on the system, assisting agencies with problems they may be experiencing with their terminals and sending All Points Broadcasts (APBDs) and informational broadcasts. Wisconsin's control center is located in the Risser Justice Center in Madison and is called the TIME System

Control Center (TSCC). If an agency needs to contact the control center, they can send an administrative message using the destination mnemonic "TSCC," or call (608) 266-7633.

TIME and Technical unit staff function as CIB's liaison with criminal justice agencies in the state of Wisconsin. In addition, the unit is responsible for conducting TIME System training and audits of those agencies with access to NCIC information.

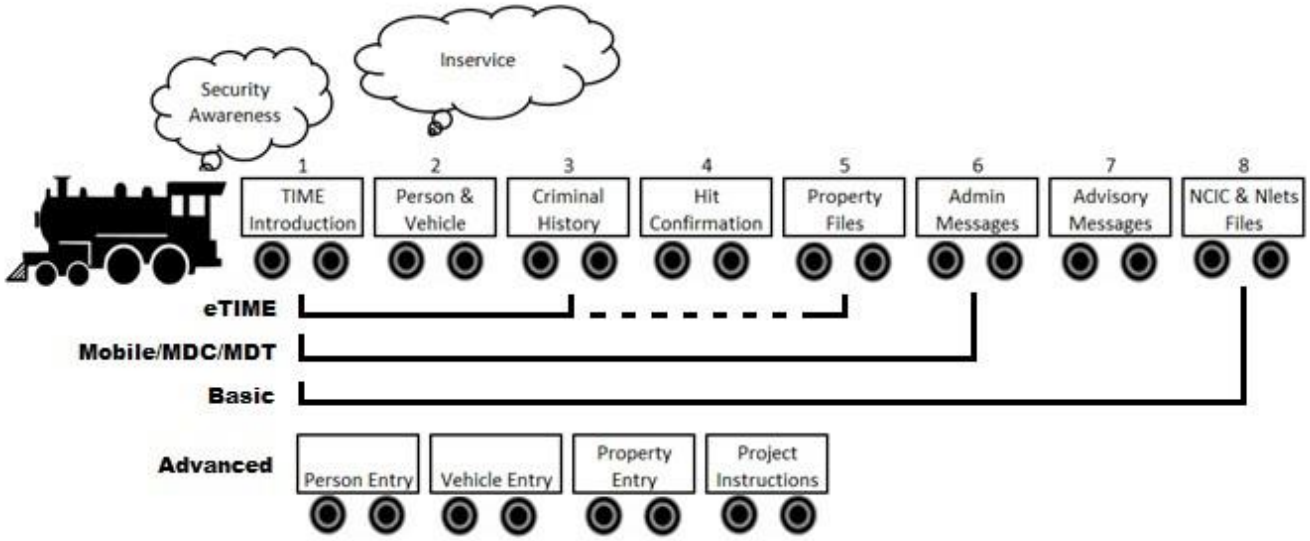
Staff members also conduct off-line searches (also called recalls) and provide analyst functions and troubleshooting for the electronic reporting of criminal history information and the TIME System.

TRAINING POLICIES

Any individual who uses a TIME System terminal must be trained in the operation of the device, system policies and procedures. In addition, all personnel with unescorted access to terminal areas and/or areas where TIME System information is stored must receive security awareness training. Initial training must occur within six months of employment or assignment to a position requiring terminal operation. This training will include a test to affirm the operator's proficiency and knowledge of CIB, NCIC and Nlets policies and procedures. All terminal operators will be re-tested biennially to reaffirm operating proficiency. The level of training should be based on system use.

TIME System Certification Levels

The Crime Information Bureau has designated five levels of training which require biennial recertification, and additional training classes that do not require recertification:



Security Awareness

This training reviews the basic security requirements that must be followed to gain access to the TIME/CJIS systems and information. It covers issues such as required background checks, physical security measures (logons, passwords, etc.), technical security requirements (encryption), and what to do in the event of a security incident. The CJIS Security policy requires that security awareness training be completed biennially by all personnel who have access to criminal justice information, manages and accesses NCIC or other CJIS systems. All employees who have access to criminal justice information and all appropriate information technology (IT) personnel shall receive security awareness within six months of their appointment or assignment. This course is designed for those who will not be attaining a TIME System certification but require security training.

Available online via TRAIN or a paper version is available on the CIB website, https://wilenet.widoj.gov/

eTIME Certification

Instruction includes TIME System query functions of the data files. Currently *e*TIME provides access to Wisconsin Department of Transportation driver's registration files and vehicle registration files, out-of-state driver's registration files and vehicle registration files, Wisconsin and out-of-state criminal history files, DOC person files, DNR files, CIB/NCIC wanted person, missing person, protection order/injunction files and other CIB/NCIC person and vehicle hot files. A query transaction is also available for CCAP, NICS and Mental Health records, CIB/NCIC stolen part file along with the NCIC stolen article, stolen security, stolen/lost/missing/felony and recovered gun files. This certification does not authorize the individual to operate mobile data computers with MDC, full query, or full access capabilities.

Available online via TRAIN only.

Online: To achieve a full *e*TIME Certification online requires completion of Modules 1, 2, 3 and 5; however, users may certify in only the modules applicable to their job duties. Student must pass test questions included in each module. Modules 1,2,3, and 5 must be completed every two years for eTIME certification.

Mobile Data Operator Certification

The training material includes file queries only; it does not include training for entries or updates. This certification authorizes the individual to operate terminals/computers with *e*TIME access, MDC access and perform transactions available for MDC's on full access terminals.

Available online via TRAIN or in a classroom environment.

Classroom: Taught by Agency Assigned Instructors (AAI). Students must pass a written examination.

Online: To achieve an MDC certification online requires completion of Modules 1 through 6. Student must pass the test included in each module.

Basic

Instruction designed for beginning personnel who access the TIME System. The training consists of basic instruction for sending administrative messages; querying the state and national computerized data files; interpretation of computer responses and security awareness. These files/responses include National Crime Information Center and Crime Information Bureau hot files of persons, vehicles, and property; Department of Corrections person files, Department of Transportation registration and licensing files; and Department of Natural Resources license and snowmobile/ATV/boat registration records. Instruction includes information on retrieving and interpreting criminal history record information from national, state, and local repositories, hit confirmation procedures and liability. Students may wish to complete the New Operator Handout prior to enrollment. A master copy of the New Operator Handout is available at https://wilenet.widoj.gov.

Available online via TRAIN or in a classroom environment.

Classroom: Instruction consists of a two-day (8:30 a.m. - 4 p.m.) session. Students must pass a written examination.

Online: To achieve a Basic certification online requires completion of Modules 1 through 8. Student must pass test questions included in each module.

Advanced

Instruction for personnel who will perform entry, modify, supplement, and cancel transactions. Training includes record entry and cancel procedures for the Warrant/Wanted and Missing Person File, Stolen Vehicle File, Stolen Part File, Gang, Threat Screening Center File, Protection Order File, Identity Theft File, Violent Person File, NICB Impound File, Detainer File, and NCIC Stolen Property Files. Modification and supplementation of data in these files are also covered. Students must successfully complete Basic Certification before attending Advanced training.

Available online via TRAIN or in a classroom environment.

Classroom: Classroom instruction consists of a two-day (8:30 a.m. - 4 p.m.) session. Students must successfully complete an "at your agency project" to achieve Advanced certification.

Online: Advanced online training consists of three (3) instructional modules and a module with materials needed to complete an "at your agency project". Students must successfully complete this project to achieve Advanced certification.

Additional TIME System Training

Inservice

Inservice training includes a review of selected TIME System topics, new or updated TIME System features and policies.

Available online via TRAIN or paper copies on WILENET.

Online: An annual inservice module is available online via TRAIN. A printable version is available on the CIB page of WILENET.

Recertification

Recertification includes an updated Security Awareness review. The recertification examination is a biennial examination for certified operators who have received Wisconsin Department of Justice certification. NCIC requires that all operators be re-certified biennially, based upon the date of their last certification.

Available online via TRAIN.

Online: An annual inservice module is available online via TRAIN. Specific recertification examinations for MDC, Basic, and Advanced operators are available online. Recertification for *e*TIME operators requires the operator recomplete the original modules 1, 2, 3 and 5 as there is no single recertification module for it.

Validation/Quality Control Training

This specialized training program is designed for individuals assigned the duty of Validation Officer and may also include supervisors. The training will include all functions of verifying computerized records; including contacting the Clerk of Courts and complainants to determine the records are still active or valid. Instruction includes an explanation of the audit program, required documentation for the audit; file validation procedures; quality control and serious error notices. Every agency validating records in the TIME/NCIC System must have a Validation Officer. CIB recommends that Validation Officers attend training every five years.

Available in a classroom environment only.

Classroom: Classroom instruction consists of a one-day (8:30 a.m. - 4 p.m.) session.

Basic Instructor Certification

This special certification is designed for persons in good standing with Criminal Justice agencies and at least three years of experience with the TIME System (Basic and Advanced Certified). This certification requires three (3) letters of recommendation from your agency administrators, a certificate of completion of an Instructor Development Course and a willingness to provide training for Basic/MDC TIME Certification for the department. Biennial re-certification is required to sustain certification. Agencies interested in additional information should contact CIB via email at CIBTRAIN@doj.state.wi.us.

TIME Agency Coordinator (TAC) Training

A specialized training program designed for persons who serve as the point of contact at their agency for matters related to TIME System access. The TAC administers the TIME System programs within the agency and oversees the agency's compliance with TIME System and FBI policies. 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 serves as the liaison between the agency and the Crime Information Bureau. The training will familiarize TIME Agency Coordinators with all physical, personnel, computer and communications safeguards and security requirements in compliance with the Department of Justice, Crime Information Bureau, Criminal Justice Information Services Division (CJIS) and International Justice and Public Safety Information Sharing Network (Nlets) rules and regulations. The TAC is responsible for ensuring terminal operators are properly trained, certified and re-certified. Instruction includes liability issues relating to the state and national files, departmental responsibilities for hit confirmation and record keeping. Every agency must designate a person as TAC and this person must complete TAC training within 12 months of assignment. CIB recommends that TACs attend training every five years

Available in a classroom environment only.

Classroom: Classroom instruction consists of a one-day (8:30 a.m. - 4 p.m.) session.

LASO Training (Local Agency Security Officer)

LASO training shall be required prior to assuming duties but no later than six months after initial assignment, and annually thereafter. At a minimum, the following topics shall be addressed as enhanced security awareness training for a LASO:

1. The roles and responsibilities listed in CJIS Security Policy Section 3.2.9.
2. Additional state/local/tribal/federal agency LASO roles and responsibilities.
3. Summary of audit findings from previous state audits of local agencies.
4. Findings from the last FBI CJIS Division audit of the CSA.
5. Most recent changes to the CJIS Security Policy.

Available online via TRAIN.

Online: An annual training module is available online via TRAIN.

CRIME INFORMATION BUREAU DATA FILES

Authorized users enter, modify, supplement, cancel and inquire on data in the CIB warrant/wanted and missing persons, stolen vehicle, part, and other assorted files using a TIME terminal. Pursuant to §165.83 and 165.84, certain warrants must be entered into the file. §342.31 requires the immediate entry as well as cancellation of all stolen motor vehicles.

Wanted Persons File

The Wanted Person File contains information regarding individuals that have outstanding court warrants or authorized wants in Wisconsin. The warrant/wanted record may also contain vehicle information associated with a wanted person. In the event an inquiry is made concerning this vehicle, the wanted person entry is also returned. The types of warrant/wanted records on file are: Felony, Temporary Felony Want, Temporary Misdemeanor Want, Non-Felony-State Law, Local Ordinance-Civil Process, State Law Violation-Civil Process, and Juvenile. Detainer information may be appended to warrant/wanted person records.

Missing Person File

The Missing Person file contains records of persons who are reported missing. Missing persons may be entered into the following categories: Disability, Endangered, Involuntary, Catastrophe Victim, Other, and Juvenile. It is closely associated with the Unidentified Person File, containing many of the same physical descriptor fields. This allows NCIC to compare records in the unidentified person file against records of missing persons for the purpose of identifying unidentified persons.

Protection Order/Injunction File

This file contains information on Temporary Restraining Orders and Injunctions. This file contains information for both the petitioner and respondent and any conditions required of the respondent.

Concealed Carry License File

This file contains information on Wisconsin residents authorized to carry concealed weapons.

Vehicle File

Information in this file includes stolen vehicles, stolen or lost license plates and vehicles used in the commission of a felony.

Stolen Part File

This file contains information regarding stolen boat and vehicle parts, provided the part has a unique identifying number permanently attached.

DEPARTMENT OF CORRECTIONS (DOC)

TIME System users have access to DOC files, including the following:

Probation & Parole File

This file contains information on juveniles and adults who are under the supervision of the Division of Probation and Parole, including currently incarcerated inmates.

Sex Offender Registration File

This file contains records of persons who have been convicted of sexual related offenses and have been ordered by the court to register.

DEPARTMENT OF NATURAL RESOURCES (DNR)

TIME System users have access to DNR files, including the following:

Customer File

This file currently contains information on persons who have been granted DNR certifications and licenses.

Citation File

This file contains information on persons who have been issued a DNR citation.

Registration File

This file contains registration information for boats, snowmobiles, all-terrain vehicles (ATV's), utility-terrain vehicles (UTV's), and off-highway motorcycles registered in Wisconsin.

CONSOLIDATED COURT AUTOMATION PROGRAM (CCAP)

CCAP provides access to certain public records of the circuit courts of Wisconsin. The information displayed is an exact copy of the case information entered into the Consolidated Court Automation Programs (CCAP) case management system by court staff in the counties where the case files are located. The court record summaries viewed are all public records under Wisconsin open records law. The information provided shows the type of case, the parties involved, and any judgment that has been entered in the case. For criminal cases, a case summary is provided to show the current pending charges or the defendant's conviction/acquittal status. A history of charges against the defendant may include criminal cases, traffic, and ordinance violations. CCAP provides the date of actions taken in a case, such as filing of the complaint or petition, pleadings, court appearances, and judgments. Individual courts vary in how much detail is entered for each court record event.

NATIONAL INSTANT CRIMINAL BACKGROUND CHECK SYSTEM (NICS)

Mandated by the Brady Handgun Violence Prevention Act of 1993 and launched by the FBI on November 30, 1998, NICS is used by Federal Firearms Licensees (FFLs) to determine whether a prospective buyer is eligible to buy firearms or explosives. Before a transfer can occur, the dealer contacts the FBI or other designated agencies to ensure the customer is eligible to purchase. In Wisconsin, handgun transfers are handled by CIB's Firearms Unit. Long gun purchases are handled by the FBI.

The NICS Index contains information provided by local, state, tribal, and federal agencies of persons prohibited from possessing firearms under federal or state law. The NICS Index contains prohibiting information which may not be found in NCIC or III databases.

NATIONAL CRIME INFORMATION CENTER (NCIC)

The FBI NCIC maintains data files of national significance. TIME System users can access these files. Many of the files maintained by NCIC are similar to files maintained by CIB at the statewide level. In addition to warrant/wanted persons, missing persons, stolen vehicles and stolen parts, NCIC files also contain:

Stolen/Lost Articles

The lost and stolen articles file is a catch all for items which are not included in other files. Examples of items included in the lost and stolen files are: bicycles, electronics equipment, livestock, toxic chemicals, and public safety, homeland security and critical infrastructure identification items (badges) and equipment, etc.

Stolen/Felony/Lost/Missing/Recovered Guns

This file contains stolen, felony, lost or missing guns identified by make, caliber, type, and serial number. If a gun has been recovered and NCIC reveals there is no want on file, the weapon can be entered into the file as a recovered gun. In the event a theft report is made later, a search will immediately reveal that the weapon has already been recovered.

Stolen Boats

This file contains stolen boats provided the vessel is registered, documented, or there is a permanent identifying serial number affixed.

Stolen/Embezzled/Missing Securities

This file contains serially numbered identifiable securities which have been stolen, embezzled, or are otherwise missing. This includes currency (paper money -- both real and counterfeit) and those documents which are traded in securities exchanges -- stocks, bonds, etc.

Unidentified Persons

This file contains records of both living and deceased unidentified persons and body parts. Many of the physical descriptors and personal property fields of this file are the same as the Missing Person File. This allows NCIC to compare records daily from the two files as an aid to identification.

Other Advisory Files

Foreign Fugitive, Gang and Threat Screening Center File Organizations, Gang members, Protective Interest, Protection Order, Immigration Violator, Supervised Release, Identity Theft, Violent Person and Sex Offender.

DEPARTMENT OF TRANSPORTATION (DOT)

TIME System users have access to DOT vehicle registration and driver information files.

Vehicle Registration File

Registration information can be obtained on passenger cars, trucks, motorcycles, trailers, motor homes and other vehicles registered in the State of Wisconsin. Information is also available on disabled person parking permits issued by DOT.

Driver's License File

This file contains driver status and driver conviction records on persons having a Wisconsin driver's license record and any non-resident having a revoked or suspended Wisconsin driver's license. Certain driver file information is confidential and protected by state and federal law.

The Federal Driver Privacy Protection Act of 2000 prohibits disclosure of personal information about any individual obtained by the Division of Motor Vehicles in connection with a Department of Transportation record**. Law enforcement and criminal justice agencies are not authorized to access this information via the TIME System when requests are made by the public.** Severe penalties may be imposed for disclosing this type of information. Form MV2896 must be completed for all requests of information from the Department of Transportation. All requests from the public for Driver/Vehicle File information should be referred to:

Wisconsin Department of Transportation
Driver Record Files
P.O. Box 7995
Madison, Wisconsin 53707-7995

Wisconsin Department of Transportation
Vehicle Record Information
PO Box 7911
Madison, WI 53707-7911

www.dot.wisconsin.gov

INTERNATIONAL JUSTICE AND PUBLIC SAFETY INFORMATION SHARING NETWORK (Nlets)

Nlets is an international telecommunications network based in Phoenix, Arizona. This network links together local, state, federal and international law enforcement, criminal justice, and public safety agencies; to enable the sharing and exchange of critical information. Nlets access enables Wisconsin agency's access to other state's driver license and vehicle registration databases, criminal history records, INTERPOL and other assorted files. Nlets users are criminal justice and authorized non-criminal justice agencies located nationwide. In Wisconsin, the CIB serves as the Nlets Control Agency.

NATIONAL INSURANCE CRIME BUREAU (NICB)

NICB maintains a rapidly expanding national and international index of records related to vehicles. This index includes manufacturer's assembly and shipping records, a record of vehicles imported and exported, thefts, impounds, salvage, auction, pre-inspection, vehicle claim, international index, vehicle lien, Mexican OCRA, eBay auction and rental. To track a motor vehicle's complete life cycle from date of manufacture to date of destruction, the database is designed to include vehicle liability, physical damage, and related homeowner claims. NICB files include data on passenger vehicles, multipurpose vehicles, trucks, trailers, motorcycles, snowmobiles, construction and farm equipment, boats, and uniquely identifiable parts.

CANADIAN POLICE INFORMATION CENTRE (CPIC)

The CPIC system is similar to NCIC. CPIC provides information to TIME System users through an Nlets interface. CPIC allows access to driver's license information and wanted person status in Canada. Included in the CPIC wanted person file are persons who are: wanted, charged, prohibited, on parole or probation, refused, under observation or missing. TIME System users can access Canadian vehicle registration information and stolen vehicle status through CPIC. Included in this file are: stolen, under observation, crime and abandoned vehicles; as well as vehicles that point to another record in the CPIC system, such as a wanted person. TIME System users also can access the following Canadian property files: articles, guns, securities, and boats. Visit the Nlets website for more information on Canadian files (Nlets: Section 32: Communicating with Canada).

Not all Canadian provinces and territories have automated drivers or vehicle files. When a province or territory is not automated, CPIC will return status information on the person's driving status. Any other needed information can be obtained by sending an administrative message to the licensing province or territory.

Canadian CHRI requests are similar to the III and state level formats. The Canadian system will return an identification segment or a full criminal record, depending on the format used for the request. The Royal Canadian Mounted Police (RCMP) has unique dissemination requirements for records transmitted internationally. Therefore, it is possible to retrieve a valid identification segment, request the full record using the Fingerprint System Number (FPS), and receive a message indicating that the requested record contains only information that cannot be disseminated outside of Canada.

INTERNATIONAL CRIMINAL POLICE ORGANIZATION (INTERPOL)

INTERPOL provides information to TIME System users through an Interface with Nlets. INTERPOL allows access to information on wanted persons, persons with criminal histories, persons connected to crimes, missing persons, stolen/lost passports and travel documents, stolen vehicles, and other law enforcement information. Law enforcement agencies can make an initial query to each of these databases to determine if a record for the subject or property exists, and then make a follow-up full query to obtain further details. When a “full query” transaction is run, in addition to returning the response to the querying agency, the system also generates a notice to the country that entered the original record and to INTERPOL in Washington D.C.

INTERPOL access requires an additional agreement between the law enforcement agency and the Crime Information Bureau prior to granting access due to additional user responsibilities.

STATUTES DEALING WITH THE TIME SYSTEM

§165.8285 Transaction information for management of enforcement system; department of corrections records.

(1) The department of justice shall, through the transaction information for management of enforcement system, provide local law enforcement agencies with access to the registry of sex offenders maintained by the department of corrections under §301.45.

§165.83 Criminal identification, records and statistics

(1) Definitions. As used in this section and §165.84

(b) “Law enforcement agency" means a governmental unit of one or more persons employed full time by the state or a political subdivision of the state for the purpose of preventing and detecting crime and enforcing state laws or local ordinances, employees of which unit are authorized to make arrests for crimes while acting within the scope of their authority.

(c) Offense" means any of the following:

1. An act that is committed by a person who has attained the age of 17 and that is a felony or a misdemeanor.
2. An act that is committed by a person who has attained the age of 10 but who has not attained the age of 17 and that would be a felony or misdemeanor if committed by an adult.
3. An act that is committed by any person and that is a violation of a city, county, village or town ordinance.

(2) The department shall:

(a) Obtain and file fingerprints, descriptions, photographs, and any other available identifying data on persons who have been arrested or taken into custody in this state:

1. For an offense which is a felony, or which would be a felony if committed by an adult.
2. For an offense which is a misdemeanor, which would be a misdemeanor if committed by an adult or which is a violation of an ordinance, and the offense involves burglary tools, commercial gambling, dealing in gambling devices, contributing to the delinquency of a child, dealing in stolen property, controlled substances or controlled substance analogs under Ch. 961, firearms, dangerous weapons, explosives, pandering, prostitution, sex offenses where children are victims, or worthless checks.
3. For an offense charged as disorderly conduct but which relates to an act connected with one or more of the offenses under sub. 2.
4. As a fugitive from justice.
5. For any other offense designated by the Attorney General.

(b) Accept for filing fingerprints and other identifying data, taken at the discretion of the law enforcement or tribal law enforcement agency involved, on persons arrested or taken into custody for offenses other than those listed in par. (a).

(c) Obtain and file fingerprints and other available identifying data on unidentified human corpses found in this state.

(d) Obtain and file information relating to identifiable stolen or lost property.

(e) Obtain and file a copy or detailed description of each arrest warrant issued in this state for the offenses under par. (a) or §346.63 (1) or (5) but not served because the whereabouts of the person named on the warrant is unknown or because that person has left the state. All available identifying data shall be obtained with the copy of the warrant, including any information indicating that the person named on the warrant may be armed, dangerous or possessed of suicidal tendencies.

(f) Collect information concerning the legal action taken in connection with offenses committed in this state from the inception of the complaint to the final discharge of the defendant and such other information as may be useful in the study of crime and the administration of justice. The department may determine any other information to be obtained regarding crime records.

(j) Compare the fingerprints and descriptions that are received from law enforcement and tribal law enforcement agencies with the fingerprints and descriptions already on file and, if the person arrested or taken into custody is a fugitive from justice or has a criminal record. Immediately notify the law enforcement and tribal law enforcement agencies concerned and supply copies of the criminal record to these agencies.

(n) Make available upon request, to all local, state and tribal law enforcement agencies in this state, to all federal law enforcement and criminal identification agencies, and to state law enforcement and criminal identification agencies in other states, any information in the law enforcement files of the department which will aid these agencies in the performance of their official duties. For this purpose, the department shall operate on a 24-hour a day basis, 7 days a week. The information may also be made available to any other agency of this state or political subdivision of this state, and to any other federal agency, upon assurance by the agency concerned that the information is to be used for official purposes only.

§165.84 Cooperation in criminal identification, records and statistics

(1) All persons in charge of law enforcement and tribal law enforcement agencies shall obtain, or cause to be obtained, the fingerprints in duplicate, according to the fingerprint system of identification established by the director of the F.B.I., full face, profile and full length photographs, and other available identifying data, of each person arrested or taken into custody for an offense of a type designated in §165.83(2) (a), of all persons arrested or taken into custody as fugitives from justice, and fingerprints in duplicate and other identifying data of all unidentified human corpses in their jurisdictions, but photographs need not be taken if it is known that photographs of the type listed, taken within the previous year, are on file at the department. Fingerprints and other identifying data of persons arrested or taken into custody for offenses other than those designated in §165.83 (2) (a) may be taken at the discretion of the law enforcement or tribal law enforcement agency concerned.

Any person arrested or taken into custody and subsequently released without charge, or cleared of the offense through court proceedings, shall have any fingerprint record taken in connection therewith returned upon request.

(2) Fingerprints and other identifying data required to be taken under sub. (1) shall be forwarded to the department within 24 hours after taking for filing and classification, but the period of 24 hours may be extended to cover any intervening holiday or weekend. Photographs taken shall be forwarded at the discretion of the law enforcement or tribal law enforcement agency concerned, but, if not forwarded, the fingerprint record shall be marked "Photo available" and the photographs shall be forwarded subsequently if the department so requests.

(3) All persons in charge of law enforcement and tribal law enforcement agencies shall forward to the department copies or detailed descriptions of the arrest warrants and the identifying data described in §165.83 (2) (e) immediately upon determination of the fact that the warrant cannot be served for the reasons stated. If the warrant is subsequently served or withdrawn, the law enforcement agency concerned must immediately notify the department of the service or withdrawal. In any case, the law enforcement or tribal law enforcement agency concerned must annually, no later than January 31 of each year, confirm to the department all arrest warrants of this type which continue to be outstanding.

(4) All persons in charge of state penal and correctional institutions shall obtain fingerprints, according to the fingerprint system of identification established by the director of the F.B.I., and full face and profile photographs of all persons received on commitment to these institutions. The prints and photographs so taken shall be forwarded to the department, together with any other identifying data requested, within 10 days after the arrival at the institution of the person committed. Full length photographs in release dress shall be taken immediately prior to the release of such persons from these institutions. Immediately after release, these photographs shall be forwarded to the department.

(5) All persons in charge of law enforcement and tribal law enforcement agencies, all clerks of court, all municipal judges where they have no clerks, all persons in charge of state and county penal and correctional institutions, and all persons in charge of state and county probation, extended supervision and parole offices, shall supply the department with the information described in §165.83 (2) (f) based on the forms and instructions to be supplied by the department under §165.83 (2) (g).

(6) All persons in charge of law enforcement and tribal law enforcement agencies in this state shall furnish the department with any other identifying data required in accordance with guidelines established by the department. All law enforcement and tribal law enforcement agencies and penal and correctional institutions in this state having criminal identification files shall cooperate in providing to the department copies of such items in these files as will aid in establishing the nucleus of the state criminal identification file.

TITLE 28 CFR, PART 20

20.33 Dissemination of criminal history record information

(a) Criminal history record information contained in the III System and Fingerprint Identification Records System (FIRS) may be made available:

1. To criminal justice agencies for criminal justice purposes, which purposes include the screening of employees or applicants for employment hired by criminal justice agencies;
2. To federal agencies authorized to receive it pursuant to federal statute or Executive order;
3. For use in connection with licensing or employment, pursuant to Public Law 92-544 (86 stat. 1115) or other federal legislation, and for other uses which dissemination is authorized by federal law. Refer to Sec. 50.12 of this chapter for dissemination guidelines relating to requests processed under this paragraph;
4. For issuance of press releases and publicity designed to affect the apprehension of wanted persons in connection with serious or significant offenses;
5. To criminal justice agencies for the conduct of background checks under the National Instant Criminal Background Check System (NICS);
6. To noncriminal justice governmental agencies performing criminal justice dispatching functions or data processing / information services for criminal justice agencies; and
7. To private contractors pursuant to a specific agreement with an agency identified in paragraphs (a)(1) or (a)(6) of this section and for providing services for the administration of criminal justice pursuant to that agreement. The agreement must incorporate a security addendum approved by the Attorney General of the United States, which shall specifically authorize access to criminal history record information, limit the use of the information to the purposes for which it is provided, ensure the security and confidentiality of the information is consistent with these regulations, provide for sanctions, and contain such other provisions as the Attorney General may require. The power and authority of the Attorney General hereunder shall be exercised by the FBI Director (or the Director's designee).

(b) The exchange of criminal history record information authorized by paragraph (a) of this section is subject to cancellation if dissemination is made outside the receiving departments or related agencies, or service providers identified in paragraphs (a)(6) & (a)(7) of this section.

(c) Nothing in these regulations prevents a criminal justice agency from disclosing to the public factual information concerning the status of an investigation, the apprehension, arrest, release or prosecution of an individual, the adjudication of charges, or the correctional status of an individual, which is reasonably contemporaneous with the event to which the information relates.

(d) Criminal history records received from the III System or the FIRS shall be used only for the purpose requested and a current record should be requested when needed for a subsequent authorized use.

20.21 Preparation and submission of a Criminal History Record Information Plan

(e) Audit

Insure that annual audits of a representative sample of state and local criminal justice agencies chosen on a random basis shall be conducted by the state to verify adherence to these regulations and that appropriate records shall be retained to facilitate such audits. Such records shall include, but are not limited to, the names of all persons or agencies to whom information is disseminated and the date upon which such information is disseminated. The reporting of a criminal justice transaction to a State, local or Federal repository is not a dissemination of information.

CIB/NCIC DATA AND PROBABLE CAUSE

A CIB or NCIC hit alone is NOT probable cause to arrest. A CIB or NCIC hit furnishes the inquirer with the fact that a stolen report, missing person report or warrant has been filed and provides the date of theft, date missing or date of warrant, which are matters to be considered by the receiving officer in arriving at an arrest decision. A hit is one fact which may be added to other facts by the officer to provide sufficient legal grounds for probable cause to make an arrest. CIB or NCIC procedure requires the inquiring agency contact the agency that submitted the record to confirm that the data is accurate and up to date. In some circumstances the confirmed hit may be the major fact, and **may be the only fact necessary** to initiate an arrest. For example when a hit on a stolen car or other stolen property is made in a time frame very close to the time of the actual theft or when a hit indicates that a car was recently used in a bank robbery or is in the possession of fugitives.

As the time period increases, the significance of the hit decreases. A hit on a record one or two years old is inadequate probable cause for an arrest since it is possible, or even probable, that the vehicle was then in the possession of an innocent purchaser, rather than the thief. To make an arrest under the latter circumstances would require that the officer not only have the fact of the hit but also additional facts adding up to probable cause. A hit confirmed with the originating agency may be adequate grounds to recover stolen property, return a missing person, or arrest a fugitive.