

## Sample TIME System Policy

### **Intent**

The rapid and efficient exchange of information between law enforcement agencies has long been recognized as one of the major necessary elements of crime control and apprehension. The Transaction Information for the Management of Enforcement (TIME) System provides a central system for the collection and dissemination of information of mutual concern to law enforcement agencies. Portions of information from the TIME System are maintained solely for reasons of officer safety.

In addition to rapid and efficient exchange of information, it is also essential that the information exchanged be accurate and complete. The TIME System is a central repository for information submitted by its contributors, who are responsible for the information entered, updated and cancelled. Each agency providing access to its files is solely responsible for the information contained therein.

The TIME System provides an efficient and expeditious means by which the procurement, exchange and transmission of information with law enforcement agencies state and nationwide is accomplished. The system also provides an effective method of administrative communication for law enforcement purposes. The TIME System is interfaced with numerous local, state and national agencies, departments and files. It is of vital importance that regulations pertaining to its use be complied with to ensure individual rights are not violated and to minimize issues of liability. Data service agencies have agreed to make information available to law enforcement and criminal justice over the TIME and NCIC Systems for the specific purpose of facilitating the administration of criminal justice. Any misuse of this information or violations of these understandings jeopardizes the availability of information for all participating agencies. The systems and the information contained therein must be protected from possible physical, natural and hardware vulnerabilities. The FBI's CJIS Security Policy establishes minimum information security requirements, guidelines and agreements reflecting the will of law enforcement and criminal justice agencies for protecting the sources, transmission, storage and generation of criminal justice information. This department has adopted the CJIS Security Policy as the department's security policy.

User agencies must also remember that data obtained from the TIME System may not be the property of the inquiring agency to release or disseminate to non-law enforcement agencies or personnel. Strict controls must be in place to ensure that improper or even unlawful release of information does not occur.

A member of the public cannot request information directly from the TIME System. If a member of the public wishes to obtain information from one of the files available via the TIME System, the requester must contact the agency that owns the file (i.e. Department of Transportation for driver's license information, CIB for Wisconsin adult criminal history, etc). Public records rules apply to requests for existing TIME System responses that were obtained in pursuance to the criminal justice / law enforcement agency's official duties and functions and are contained within agency case files. The TIME System interfaces with data files maintained by various data sources. The ability to re-disclose information obtained from the TIME System, in response to a public records request for existing records, depends on: 1) Any restrictions imposed by the data source or applicable law, and 2) Your usual public records analysis. An agency may need to redact non-disclosable confidential data prior to release. Additional information on which data sources restrict or limit re-disclosure is available on the TIME System manual found at <http://www.doj.state.wi.us/dles/cibmanuals>.

As a subscriber/user of the TIME System, this agency has agreed to utilize the system for official purposes only. If TIME System data is provided to other authorized agencies, a signed agency agreement will be obtained with those agencies.

## **Probable Cause**

A TIME System hit alone is NOT probable cause to arrest. A TIME System hit furnishes the inquirer the fact that a stolen report, missing person report or warrant has been filed and also 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 that must be added to other facts by the officer in arriving at sufficient legal grounds for probable cause to arrest. Correct procedure demands that the agency which placed the record in the file be contacted by the inquiring agency to confirm that the data is accurate and up to date. In some circumstances the hit confirmed with the originating agency may be the major fact, and indeed, may be the only fact necessary; for instance 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. Thus, a hit on a record a year or two years after the car had been stolen would in itself be inadequate probable cause for an arrest since it would be 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.

## **TIME Agency Coordinator**

This agency will designate an employee of this agency to serve as TIME Agency Coordinator (TAC). The TAC will be responsible for coordinating training of the functions of the terminal, ensuring compliance with National Crime Information Center (NCIC) and Crime Information Bureau (CIB) policy and regulations including validation and other requirements, and format training in conjunction with CIB certification, re-certification and specialized training classes. The TAC will attend CIB TIME System TAC training within one year of appointment as TAC.

## **Security**

Each TIME System agency is responsible for allowing only authorized personnel to operate the TIME terminal and enforce system and data security. As part of this responsibility, each terminal agency is responsible for ensuring that the terminal is used to send authorized and official messages only. Any violation of this TIME System policy or misuse of information obtained from the TIME System will subject personnel to any and/or all departmental disciplinary procedures. Any department member who witnesses or has knowledge of a violation of TIME System access or other section of this policy is required to report this violation to a supervisor. A FBI authorized Originating agency Identifier (ORI) assigned to this agency shall be used in each transaction.

### ***System Usage***

Users should 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/criminal justice personnel for law enforcement/criminal justice purposes. Each criminal justice agency

authorized to access the TIME/NCIC Systems shall 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, individuals and agencies may be subject to criminal/other penalties.

Any individual authorized to use the TIME System who receives a request for TIME System information from another individual must ensure the person requesting the information is authorized to receive the data. 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.

Records obtained via the TIME/NCIC systems must be stored in a secure records environment, inaccessible to the public. All records must be properly disposed of by shredding, incineration, degaussing or another appropriate secure method. Re-disclosure of an existing TIME System response contained within a file of this criminal justice agency, when that file is subject to a public records request, must comply with re-disclosure restrictions for data sources, the Wisconsin Public Records Law and other applicable law.

### ***Physical Security***

The following physical protection policies and procedures will be implemented to ensure criminal justice information and information system hardware, software and media are physically protected through access control measures.

#### **Physically Secure Location**

A physically secure location is a criminal justice facility, an area, a room, a group of rooms that is/are subject to criminal justice agency management control. For interim compliance, and for the sole purpose of meeting the advanced authentication policy, a police vehicle is considered a physically secure location until September 30<sup>th</sup> 2013. For the purposes of this policy, a police vehicle is defined as an enclosed criminal justice conveyance with the capability to comply with physical access authorizations.

#### **Security Perimeter**

The perimeter of this agency's physically secure locations will be prominently posted and separated from non-secure locations.

#### **Physical Access Authorizations**

This agency will develop and keep current a list of personnel with authorized access to the physically secure location (except for those areas within the permanent facility officially designated as publicly accessible) or shall issue credentials to authorized personnel.

#### **Physical Access Control**

This agency will control all physical access points (except for those areas within the permanent facility officially designated as publicly accessible) and will verify individual access authorizations before granting access.

#### **Access Control for Transmission Medium**

This agency will control physical access to information system distribution and transmission lines within the physically secure location.

#### **Access Control for Display Medium**

This agency will control physical access to devices that display criminal justice information and will position information system devices in such a way as to prevent unauthorized individuals from accessing and viewing criminal justice information.

#### **Monitoring Physical Access**

This agency will monitor physical access to the information system to detect and respond to physical security incidents.

#### **Visitor Control**

This agency will control physical access by authenticating visitors before authorizing escorted access to the physically secure location (except for those areas designated as publicly accessible). This agency will escort visitors at all times and monitor visitor activity.

#### **Access Records**

This agency will maintain visitor access records to the physically secure location (except for those areas designated as publicly accessible) that include:

- Name and agency of the visitor.
- Signature of the visitor.
- Form of identification.
- Date of access.
- Time of entry and departure.
- Purpose of visit.
- Name and agency of person visited.

Designated officials within this agency will frequently review the visitor access records for accuracy and completeness. The visitor access records will be maintained for a minimum of one year.

#### **Delivery and Removal**

This agency will authorize and control information system-related devices entering and exiting the physically secure location.

### ***Identification and Authentication***

This agency will identify information system users and processes acting on behalf of users and authenticate the identities of those users or processes as a prerequisite to allowing access to agency information systems or services.

### **Identification Policy and Procedures**

Each individual who is authorized to store, process, and/or transmit criminal justice information will be uniquely identified. A unique identification will 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 take the form of a full name, badge number, serial number, or other unique alphanumeric identifier. This agency will require users to identify themselves uniquely before the user is allowed to perform any actions on the system. This agency will ensure that all user IDs belong to currently authorized users. Identification data will be kept current by adding new users and disabling and/or deleting former users.

### **Use of Originating Agency Identifiers in Transactions and Information Exchanges**

An FBI authorized Originating Agency Identifier (ORI) will be used in each transaction to identify the agency / user making the request to ensure the proper level of access for each transaction.

### **Standard Authentication (Password)**

This agency will follow the secure password attributes listed below to authenticate an individual's unique ID. Passwords will:

- Be a minimum length of 8 characters on all systems.
- Not be a dictionary word or proper name.
- Not be the same as the Userid.
- Expire within a maximum of every 90 calendar days.
- Not be identical to the previous ten (10) passwords.
- Not be transmitted in the clear outside the secure location.
- Not be displayed when entered.

### **Advanced Authentication**

Advanced authentication provides for additional security to the typical user identification and authentication of login ID and password, such as: biometric systems, user-based public key infrastructure (PKI), smart cards, software tokens, hardware tokens, paper (inert) tokens, or "Risk-based Authentication" that includes a software token element comprised of a number of factors, such a network information, user information, positive device identification (i.e. device forensics, user pattern analysis and user binding), user profiling and high-risk challenge/response questions. The requirement to use or not use advanced authentication is dependent upon the physical, personnel and technical security controls associated with the user location.

## ***Personnel Security***

### **Background Screening**

Thorough background screening by this agency of personnel is required. State and national criminal history record checks by fingerprint identification must be conducted within 30 days upon initial employment or assignment for all personnel who have authorized access to FBI CJIS Systems and those who have direct responsibility to configure and maintain computer systems and networks with direct access to FBI CJIS Systems. The minimum check must include submission of completed applicant fingerprint cards to the FBI CJIS Division and the CIB through the state identification bureau. CIB and NCIC Wanted Person Files must also be checked. Sworn personnel who have been fingerprinted and certified by the law enforcement standards board already meet this requirement. Background re-investigations are recommended every 5 years as good business practice.

When identification of the applicant or employee has been established by fingerprint comparison and he/she appears to be a wanted person or to have an arrest history for a felony or serious misdemeanor, this agency must delay granting NCIC access until the matter is reviewed by the CJIS Systems Officer (CSO) or designee. If a felony conviction of any kind exists, the hiring authority in this agency will deny systems access. However, the hiring authority may ask for a review by the CSO in extenuating circumstances where the severity of the offense and the time that has passed would support a possible variance. Other offenses may be disqualifying at the discretion of this agency or the CSO. (Note: A denial of NCIC access may not be sufficient grounds for denial of employment. This agency must consider the provisions of Chapter 111, Wisconsin Statutes, relating to employment discrimination). If the person already has access to CJIS systems and is subsequently arrested and or convicted, continued access to CJIS will be determined by the CSO.

### ***Technical Security***

Each agency having access to CJIS data through their own network must complete and submit an Interface Application for approval and designate someone as the Local Agency Security Officer (LASO). The LASO will be responsible for the following:

- Identifying who is using the CSA approved hardware / software / firmware and ensure that no unauthorized individuals or processes have access to the same.
- This agency will ensure that a complete topological drawing depicting the interconnectivity of the agency network, to criminal justice information, systems and services is maintained in a current status. The network topological drawing will include the following:
  - All communication paths, circuits and other components used for the interconnection, beginning with our agency owned system(s) and traversing through all interconnected systems to our agency end-point.
  - The logical location of all components (e.g. firewalls, routers, switches, hubs, servers, encryption devices and computer workstations). Individual workstations (clients) do not have to be shown; the number of clients is sufficient.
  - "FOR OFFICIAL USE ONLY" markings.
  - This agency's name and date (day, month, and year) drawing was created or updated.
- Ensure that personnel security screening procedures are being followed as stated in this policy.

- Ensuring the approved and appropriate security measures are in place and working as expected.
- Supporting policy compliance and ensure the CSA / ISO is promptly informed of security incidents.

All CJIS data transmitted through any public network segment or over dial-up, wireless or Internet connections will be protected with a minimum of 128 bit encryption with NIST, CSL certification of the cryptographic module to ensure that it meets FIPS Publication 140-2 for "Security Requirements for Cryptographic Modules". This requirement also applies to any private data circuit that is shared with non-criminal justice users and/or is not under the direct management control of a criminal justice agency.

All CJIS data transmitted over dial-up, wireless or Internet connections must include Advanced Authentication such as: Biometrics Systems, User-based Public Key Infrastructure, Smart Cards, Token Devices or Risk-based Authentication.

### **Media Protection**

Access to electronic and physical media in all forms is restricted to authorized individuals. The following procedures are defined for securely handling, transporting and storing media.

- **Media Storage and Access**

This agency will securely store electronic and physical media within physically secure locations or controlled areas. This agency will restrict access to electronic and physical media to authorized individuals.

- **Media Transport**

This agency will protect and control electronic and physical media during transport outside of controlled areas and restrict the transport of such media to authorized personnel.

- **Electronic Media Sanitization and Disposal**

This agency will sanitize or degauss electronic media prior to disposal or release for reuse. Inoperable electronic media will be destroyed (cut up, shredded, etc.). This agency will maintain written documentation of the steps taken to sanitize or destroy electronic media. This agency will ensure the sanitization or destruction is witnessed or carried out by authorized personnel.

- **Disposal of Physical Media**

Physical media will be securely disposed of when no longer needed. Physical media will be destroyed by shredding, incineration, etc. This agency will ensure the disposal or destruction is witnessed or carried out by authorized personnel.

### ***Access Control***

Access control provides the planning implementation of mechanisms to restrict reading, writing, processing and transmission of CJIS information and the modification of information

systems, applications, services and communication configurations allowing access to CJIS information.

### **Account Management**

This agency will manage information system accounts (establishing, activating, modifying, reviewing, disabling and removing accounts). This agency will validate information system accounts at least annually and will document the validation.

### **Least Privilege**

This agency will approve individual access privileges and will enforce physical and logical access restrictions associated with changes to the information system; and generate, retain and review records reflecting all such changes. This agency will assign the most restrictive set of rights/privileges or access needed by users for the performance of specific tasks. This agency will implement least privilege based on specific duties, operations or information systems as necessary to mitigate risk to criminal justice information.

Logs of access privilege changes will be maintained for a minimum of one year or at least equal to this agency's record retention policy – whichever is greater.

### **Access Control**

Access controls will be in place and operational for all IT systems to:

- Prevent multiple concurrent active sessions for one user identification, for those application accessing criminal justice information, unless this agency grants authority based upon operational business needs. This agency will document the parameters of the operational business needs for multiple concurrent active sessions.
- Ensure only authorized personnel can add, change or remove component devices, dial-up connections and remove or alter programs.
- This agency will control access to criminal justice information based on one or more of the following: job assignment or function, physical location, logical location, network addresses, time-of-day and day-of-week/month.
- Access controls will use one or more of the following: Access Control Lists (ACLs), resource restrictions (i.e. menus, database views and network devices), encryption or controlling access at the application level.

### **Unsuccessful Login Attempts**

Where technically feasible, the system will enforce a limit of no more than 5 consecutive invalid access attempts by a user (attempting to access criminal justice information or systems with access to criminal justice information). The system will automatically lock the account for at least a 10 minute period unless released by an administrator.

### **Session Lock**

The information system will 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. Users can directly initiate session lock mechanisms to prevent inadvertent viewing when a device is unattended. A session lock is not a substitute for logging out of the information system. In the interest of officer safety, devices that are: (1) part of a police vehicle; or (2) used to perform dispatch functions and located within a physically secure location, are exempt from this requirement. Note: an example of a session lock is a screen saver with password.

### **Publicly Accessible Computers**

Utilizing 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.

## **System & Communications Protection & Information Integrity**

Examples of systems and communications safeguards range from boundary and transmission protection to securing this agency's virtualized environment. In addition, applications, services or information systems must have the capability to ensure system integrity through the detection and protection against unauthorized changes to software and information.

### ***Information Flow Enforcement***

The network infrastructure will control the flow of information between interconnected systems. Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. In other words, controlling how data moves from one place to the next in a secure manner. Examples of controls are:

- Prevent criminal justice information from being transmitted unencrypted across a public network.
- Block outside traffic that claims to be from within the agency.
- Do not pass any web requests to the public network that are not from the internal web proxy.

### **Encryption**

- Encryption will be a minimum of 128 bit.
- When criminal justice information is transmitted outside the boundary of the physically secure location, the data will be immediately protected via cryptographic mechanisms (encryption).
- When encryption is employed, the cryptographic module used will be certified to meet FIPS 140-2 standards.
- If this agency is using public key infrastructure technology, this agency will develop and implement a certificate policy and certification practice statement for the issuance of public key certificates used in the information system. Registration to receive a public key certificate will:
  - Include authorization by a supervisor or a responsible official.

- Be accomplished by a secure process that verifies the identity of the certificate holder.
- Ensure the certificate is issued to the intended party.

### **Patch Management**

This agency will identify applications, services and information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws.

### **Malicious Code Protection**

This agency will implement malicious code protection that includes automatic updates for all systems with Internet access. If this agency's system is not connected to the Internet it will implement local procedures to ensure malicious code protection is kept current (i.e. most recent update available).

This agency will employ virus protection mechanisms to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses) at critical points throughout the network and on all workstations, servers and mobile computing devices on the network. This agency will ensure malicious code protection is enabled on all of the aforementioned critical points and information systems and resident scanning is employed.

### **Spam and Spyware Protection**

This agency will implement spam and spyware protection. This agency will:

- Employ spam protection mechanisms at critical information system entry points (e.g., firewalls, electronic mail servers, remote-access servers).
- Employ spyware protection at workstations, servers or mobile computing devices on the network.
- Use the spam and spyware protection mechanism to detect and take appropriate action on unsolicited messages and spyware/adware, respectively, transported by electronic mail, electronic mail attachments, Internet accesses, removable media (e.g., diskettes or compact disks) or other removable media.

### **Personal Firewall**

A personal firewall will be employed on all devices that are mobile by design (i.e. laptops, handhelds, personal digital assistants, etc.). For the purpose of this policy, a personal firewall is an application that controls network traffic to and from a computer, permitting or denying communications based on policy. At a minimum, the personal firewall will perform the following activities:

- Manage program access to the Internet.
- Block unsolicited requests to connect to the PC.
- Filter Incoming traffic by IP address or protocol.
- Filter Incoming traffic by destination ports.
- Maintain an IP traffic log.

### ***Incident Response***

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.

This agency will promptly report incident information to the Crime Information Bureau. Information security events and weaknesses associated with information systems will be communicated in a manner allowing timely corrective action to be taken. Formal event reporting and escalation procedures will be in place. Wherever feasible, the agency will employ automated mechanisms to assist in the reporting of security incidents. All employees, contractors and third party users will be made aware of the procedures for reporting the different types of events and weaknesses that might have an impact on the security of agency assets and are required to report any information security events and weaknesses as quickly as possible to the designated point of contact.

### ***Data Security***

Data stored in central repositories such as CIB and NCIC files must be protected from unauthorized access and access is restricted to authorized agencies. Data stored in the databases of participating data service agencies are documented justice records or administrative records containing sensitive personal information. These records must be protected to ensure correct, legal and efficient dissemination and use. Each data service has its own rules for secondary dissemination of records.

Information accessed via the TIME System shall be used only for the purpose for which the request was made. Access is subject to cancellation if information is improperly disseminated. The TIME System will not be used to obtain data for personal reasons. The selling of information obtained from the TIME System is strictly prohibited, and illegal.

This agency accesses TIME System files, but is not the custodian of the records contained in those files. Any public access request for release of those records should be made to the custodian of those records, i.e., the Department of Transportation (DOT), CIB, etc. This department will release data obtained via the TIME System only to those law enforcement/criminal justice agencies with which this department has a signed agreement detailing dissemination of that information and immediate notification of updated information.

### **Department of Transportation records**

The Wisconsin DOT is the custodial agency for vehicle and driver record information obtained via the TIME System and dissemination of information is the responsibility of the custodial agency. DOT provides access to this information via the TIME System for the use of law enforcement/criminal justice agencies only. The federal Driver Privacy Protection Act (18 USC s. 2721) permits use of personal information from state motor vehicle records or use by any government agency, including any court or law enforcement agency, in carrying out its functions, along with other permitted uses for such information. TIME System access to these files is for law enforcement purposes only due to the confidentiality of many of the record entries. The requirement for completion of the Federal Driver Privacy Protection Act (DPPA) (MV2896) form makes it necessary for other persons or agencies to deal directly with DMV.

- **Vehicle registration files**

This department will advise any person that public requests for registration information can be obtained by completing the appropriate form, paying the appropriate fees, enclosing a self addressed stamped envelope and contacting:

Wisconsin Department of Transportation  
Vehicle Records Section  
PO BOX 7911  
Madison, WI 53707-7911

Further information and forms are also available on the DOT website [www.dot.wisconsin.gov/drivers/forms.pdf](http://www.dot.wisconsin.gov/drivers/forms.pdf). The same guidelines used for vehicle registration apply to other registration information available on the TIME System such as boats, snowmobiles, etc. This department is not the custodian of those records and therefore will not release those records to the public. Likewise, information as to whether or not the vehicle or other items queried through the TIME System is wanted or stolen will not be released to the public, however the information may be broadcast for the purpose of apprehension/identification or officer safety reasons.

- **Driver's license files**

This department will advise any person that public requests for driver license information can be obtained by completing the appropriate form, paying the appropriate fees, enclosing a self addressed stamped envelope and contacting:

Wisconsin Department of Transportation  
Driver Record Section  
PO BOX 7995  
Madison, WI 53707-7995

Further information and forms are also available on the DOT website [www.dot.wisconsin.gov/drivers](http://www.dot.wisconsin.gov/drivers). Warrant/wanted or missing status shall not be released to the public, however may be broadcast for the purpose of apprehension/identification or officer safety reasons.

- **Juvenile record information**

Wisconsin statutes state DOT shall not disclose juvenile records concerning or related to certain violations to any person other than a court, district attorney, county corporation counsel, city, village or town attorney, law enforcement agency, the minor who committed the violation or their parent/guardian. This information is present on driver record checks made by law enforcement/criminal justice agencies via the TIME System. It is necessary that it not be divulged to anyone other than those listed above, and is for the internal use of such agencies only. These entries will be listed as 'confidential.' These entries include but are not limited to juvenile alcohol violations and failure to pay juvenile forfeiture violations. Confidential entries should not be released or broadcast on

an open radio frequency, unless, for some reason, there is an entry that involves officer safety.

**Criminal history record information**

Criminal History Record Information (CHRI) means information collected by criminal justice agencies on individuals, consisting of identifiable descriptions and notations of arrests, detentions, indictments, information or other formal criminal charges and disposition arising therefrom, sentencing, correctional supervision and release.

CHRI must be afforded strict privacy consideration by law enforcement/criminal justice agencies. Requests for CHRI must be submitted in the proper format specified by CIB/NCIC. This format requires that each request for CHRI utilize the proper purpose code(s) and identification of the specific individual requesting/receiving the CHRI. This ensures prohibited information is not released to unauthorized persons. CHRI requests are subject to audit and therefore must be able to be tracked within the department as to final destination and reason for the request.

Individuals wishing a copy of their record from CIB or the FBI, or other public requests for CHRI will be directed to either CIB or the FBI, as appropriate. Persons requesting Wisconsin CHRI may receive Wisconsin adult criminal history record information under the provisions of the Wisconsin open records law. Information can be obtained by completing the appropriate form, paying the appropriate fees, enclosing a self addressed stamped envelope and contacting:

Wisconsin Department of Justice  
Crime Information Bureau  
Record Check Unit  
PO Box 2688  
Madison, WI 53701-2688

Further information and forms are also available on the DOJ website. The Department also provides for online access to this information, and public requestors may also be directed to the website at [www.doj.state.wi.us/dles/cib](http://www.doj.state.wi.us/dles/cib).

III shall not be used to access a record to be reviewed and/or challenged by the subject of the record. If an individual has a criminal record maintained by the FBI and the record has been entered into III, it is available for review through the FBI, upon presentation of the appropriate fee and identification (which includes a set of rolled fingerprint impressions, name, date and place of birth). A written request must be submitted to:

FBI-CJIS Division  
ATTN: SCU Module D-2  
1000 Custer Hollow RD  
Clarksburg, WV 26306-0171

o **Attention line**

Requests for CHRI must be submitted in the proper format specified by CIB/NCIC. This format requires that each request for CHRI identify the specific individual receiving the CHRI information. Include the unique identifier of the

specific individual the segment/record will be given to (e.g., Lt. Smith, Officer Jones, DA Johnson). If space permits, the attention line should also include either a case number or text providing the reason for the inquiry.

○ **Purpose codes**

Requests for CHRI must be submitted in the proper format specified by CIB/NCIC. This format requires that each request for CHRI utilize the proper purpose code(s). Authorized purpose codes include the following:

▪ ***Purpose code C***

Criminal justice/law enforcement purposes. Purpose code C is accepted by CIB and the Interstate Identification Index (III). Adult and juvenile records will be supplied. This code is used for official duties in connection with the administration of justice. This includes detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision or rehabilitation of accused persons or criminal offenders. A criminal history record check may also be made using purpose code C for the purposes of the security of a criminal justice facility. This may include checks on vendors, contractors, volunteers at the criminal justice agencies not involved in the administration of criminal justice, or participants of law enforcement sponsored firearms training class held at a public firing range or law enforcement facility. Confinement facility visitors and inmate mailing lists also meet this criterion.

▪ ***Purpose code J***

Criminal justice/law enforcement employee applicants. Purpose code J is accepted by CIB and III. Adult and juvenile records will be supplied.

▪ ***Purpose code D***

Domestic violence and stalking. Purpose code D is accepted by CIB and III. CIB will return only adult records. III will return information that has not been sealed by the contributing state. Civil court cases involving domestic violence or stalking cases (civil courts are issued a NCIC Agency Identifier with the letter D in the ninth position of the identifier). Law enforcement agencies providing CHRI to a criminal or civil court for a domestic violence hearing.

▪ ***Purpose code H***

Public housing applicants. Purpose code H is accepted by CIB and III. CIB will return only adult records. III will return an identification response only. Purpose code H is used to check the suitability of applicants for public housing under the authority of the Housing Opportunity Extension Act of 1996. If a complete record is requested the Public Housing Authority must submit a fingerprint card to the Federal Bureau of Investigation (FBI). There is a fee associated with a CHRI request made using this purpose code.

- ***Purpose code F***

Return of firearms to a lawful owner. Purpose code F is accepted by CIB and III. Both adult and juvenile records will be returned. Purpose code F is to be used by criminal justice agencies in possession of firearms that have been stolen, confiscated or used in suicides who are concerned that in returning such firearms to their lawful owner(s) the agency may be providing firearms to persons who are prohibited by federal or state law from possession of firearms. This code may also be used in cases where the firearm is pawned.

- ***Purpose code E***

Other authorized employment or licensing purposes. Purpose code E is accepted by CIB only. III does not accept this purpose code, and no other purpose code may be used when requesting CHRI for purpose of licensing/non-criminal justice employment. No other legitimate purpose code may be used to bypass the built in safeguards preventing the use of III information for licensing. Only adult records will be returned. Authorized means that the criminal history inquiry is required by state statutes, local ordinance or federal regulation. There is a fee associated with a CHRI request made using this purpose code.

- **Secondary dissemination**

This agency accesses CHRI, but is not the custodian of the records contained in those files. This department will release data obtained via the TIME System only to those law enforcement/criminal justice agencies with which this department has a signed agreement detailing dissemination of that information and immediate notification of updated information. If CHRI is released to another authorized user of such information, and that user was not specifically identified in the attention line of the CHRI request, the department will log such dissemination. The reporting of a criminal justice transaction to a state, local or federal repository is not a dissemination of information. This log will include a notation of what information was disseminated, whom the information was disseminated to, and the date of the dissemination. This log shall be maintained for a minimum of one year, and will be made available for review by NCIC/CIB auditors upon request.

- **Storage of CHRI information**

CHRI records obtained by a law enforcement/criminal justice agency via the TIME System become a local agency record and may be subject to release under the Wisconsin open records law. These records may not necessarily be up to date and accurate when the request for information from the case file is made, therefore CHRI records will not be maintained in case files. Criminal history records received from the III System or the Fingerprint Identification Records Section (FIRS) will be used only for the purpose requested and a current record should be requested when needed for a subsequent authorized use. Identifiers obtained from CHRI may be maintained in the file, but the actual criminal record

will be disposed of once the case has been forwarded to the prosecuting attorney, or if not forwarded, when the case is closed or no longer actively under investigation.

## **Training**

Trained personnel are more effective and efficient in the performance of their assigned TIME System responsibilities. In addition, having untrained personnel may subject an agency to potential liabilities. As a TIME System user, this agency has agreed to participate in a system of TIME System operator training and re-certification.

### ***Initial training***

Each individual using the TIME System or information received via the TIME System will be trained in the operation of equipment, system policies and procedures. This includes field and office personnel that use the system only to relieve terminal operators. The level of training will be based on system use. Initial training will occur within six months of employment or assignment to a position with TIME System access privileges. This training will include a test to affirm the operator's proficiency and knowledge of data services connected to the TIME System. Security awareness training is incorporated into the standard TIME System certification level training, but is also available in a separate online module for those personnel that do not require TIME System certification. Prior to this initial training, all TIME terminal users shall read/complete the new operator training.

### ***Re-certification***

All TIME System users will be retested biennially to reaffirm operating proficiency. Re-certification must be accomplished by the operator's anniversary date. All operators shall maintain their certification and employees without valid certification will not be allowed to work as a TIME System operator. All personnel who access the TIME System will keep up-to-date on any TIME System changes by reading the TIME System newsletters published by CIB.

## **Data File Entries**

As a user/participant in the TIME System, this agency is provided the opportunity to make entries into various statewide and nationwide databases listing wanted persons, missing persons, stolen property, etc. Other law enforcement/criminal justice personnel throughout the state and country view information entered into such files by this agency. Entries to these files must be accurate, complete and valid/up-to-date. To meet these goals this agency adopts the following guidelines for data entry:

### ***When to Make a Data File Entry***

To ensure maximum system effectiveness, entry into the data files should be made immediately upon receipt of required documentation and minimum data required for entry, not to exceed three days of receipt of information. The only exceptions to immediate entry are when otherwise prescribed by law. Although data entries may be made with minimum data, it is the policy of this department to enter as much information as is available. If data becomes available at a later date, the record may be updated to include the new information.

Inquiries should be made to the TIME System DOT files, CHRI files, Department of Natural Resources files, etc., the department's in-house computer system and any other existing records to obtain all the data available. Any new information should be retained with the original case file to show where the identifiers/new information was obtained. Any information that cannot be verified will not be included in the data entry.

### ***Quality Control***

In an effort to make sure data file entries do not contain errors, it is the policy of this department to have the data file entry checked by another department member. The member verifying the accuracy of the data should initial the entry. All updates to entries (modification, supplement) are also subject to this second party check procedure.

### ***Images***

The TIME System supports entry of NCIC images for persons, articles, parts, boats and vehicles. Authorization must be obtained from the source of the image to use the image as an attachment to any TIME System entry. This agency will enter an image when there is one available for the person or property or and there is investigative value in doing so. To enter an image the base record must already exist.

### ***Documentation Required for Entry***

Entry of data in the TIME System can only be accomplished if the entering agency has proper documentation in its possession. Each piece of information must be supported by documentation and this documentation must be available for review by CIB/NCIC auditors. Case files will be available 24 hours a day and all operators will know and have access to where the case record can be located. If the case file is removed from where it is routinely stored it will be replaced with an insert card to note when the file was removed, who removed it and where it can be found. Examples of suitable documentation for the various files are listed in the following sections. The list of examples is not all-inclusive, but merely a reference.

#### **Warrant/Wanted Person File**

Must possess a court issued warrant or have an investigative report sufficient to obtain a warrant and show that because of extenuating circumstances we have been unable to obtain the warrant. Entries into this file are based upon the following warrant categories, with the actual offense specified in the entry.

- **Categories**

- ***Felony***

- This category is used when the charge is a violation of state law that calls for a penalty of imprisonment in state prison (Ss 939.60). The warrant can be entered into CIB only or CIB and NCIC.

- ***Temporary Felony Want***

- This category is used when law enforcement needs to take prompt action to

apprehend a person who is alleged to having committed a felony. The individual may seek refuge by fleeing across jurisdictional boundaries while circumstances prevent the immediate acquisition of a warrant. A warrant for the arrest of the individual must be obtained as soon as possible. This entry requires knowledge by law enforcement that a felony was committed and who the person was that committed the felony but no warrant has been issued yet. This record can be entered and will remain on the files for 48 hours and then will be automatically purged. The want can be entered into CIB only or CIB and NCIC.

- ***Non-Felony State Law Violation Warrant***

This category is used for entries that are misdemeanors, criminal traffic warrants, etc. when the charge is based on a violation of state statute that is punishable by fine and/or time in county jail for a period of less than one year. The warrant can be entered into CIB only or CIB and NCIC.

- ***Temporary Misdemeanor Want***

This category is used when law enforcement needs to take prompt action to apprehend a person who is alleged to having committed a misdemeanor. The individual may seek refuge by fleeing across jurisdictional boundaries while circumstances prevent the immediate acquisition of a warrant. A warrant for the arrest of the individual must be obtained as soon as possible. This category requires knowledge by law enforcement that a misdemeanor was committed and who the person was that committed the misdemeanor but no warrant has been issued yet. This record can be entered and will remain on the files for 72 hours and then will be automatically purged. The want can be entered into CIB only.

- ***Civil Process Non-Criminal State Law Violation Warrant***

This is a violation of state law or statute but the penalty calls for a forfeiture instead of a fine or imprisonment. Restrictions can be applied on distance of service. The warrant can be entered into CIB only.

- ***Civil Process Local Ordinance Violation Warrant***

This is a violation of an ordinance. An ordinance is defined as a regulation adopted by the governing body of a city, town or county. Because an ordinance violation is a civil violation and not a crime, restrictions on service can be applied against an ordinance violation warrant. The restriction to how far the Police Agency will travel to serve the warrant is allowed on an ordinance or civil process violation. The warrant can be entered into CIB only.

- ***Juvenile Warrant***

This is for a person under 17 years of age who has been declared delinquent by a juvenile court. The warrant can be entered into CIB only or CIB and NCIC.

- **Extradition/Geographic Restrictions**

Before entering a record of a wanted person into the NCIC files, the entering agency must attempt to determine, to the maximum extent possible, if extradition will be authorized if the individual is located in another state. If extradition is not authorized, the entry still may be entered into NCIC if the notation 'NOEX' is listed as the first four characters in the remarks field or Extradition Code "04" (No Extradition) in the Extradition Limitation Field. Entry of such non-extraditable warrants provides notice to law enforcement/criminal justice in other states of the wanted subject's status and provides important officer safety information. This agency will not make entries to the NCIC wanted persons file unless the case file includes evidence of communication with the district attorney's office indicating whether or not they will extradite, and what limitations they place on that extradition.

If a warrant/wanted subject entry is subject to any other geographic restriction, either upon order by the court or other agency policy, such geographic restrictions will be listed on the entry to provide other criminal justice agencies with needed information regarding our agency's intention to retrieve the wanted subject when located. If the geographic restriction is court ordered the restriction must be listed/further explained in the remarks of the entry.

CIB policy allows for the entry of court ordered geographic restrictions. CIB also permits the entry of local ordinance and state law-civil process violations with an agency assigned geographical pickup restriction. Agencies that enter ordinance or civil process warrants but are not willing to travel statewide to pick up the subject based on bond amount or seriousness of the offense, must geographically restrict the entry so agencies that receive a positive response will not detain the person unless they are within the restricted boundaries. Warrants for non-felony state law violations may only be geographically restricted by the court. CIB recommends that agencies establish internal policies regarding agency assigned geographic restrictions.

- **Detainers**

The detainer file allows an agency warrant/wanted person record to remain entered after hit confirmation has occurred, but the arrested subject will not be released to the agency holding the warrant. Detainer information is appended to the already existing warrant/wanted person record and can only be placed on a record that has a locate placed on it. This information may include details of where the subject is being held, how long he will be held, and miscellaneous remarks. There will be times when the conditions of the sentence will change and/or multiple agencies will have warrants for the same subject. When this occurs, the detainer must be modified with each change of sentence and/or place of incarceration. If detainer information is appended to a record, the agency must maintain documentation of the information listed in the detainer.

The ending date must be a documented date accurately representing the anticipated transfer of the subject by the incarcerating agency to your department. The requirement of the ending date field as mandatory was designed to automatically clear old records by purging them after this date. If a record

containing detainer information is audited during a biennial audit and found to contain an undocumented or inaccurate ending date it will be counted as wrong the same as any other record containing fictitious/undocumented data.

If the subject is not immediately available for pick up and the agency is unable to determine the ending date at the time of entering the detainer information, a date of 10 days or less may be entered as the ending date. This will then generate the automatic messages to both the incarcerating agency and the entering agency at approximately 0000 hours of the ending date. This allows the incarcerating and entering agency 24 hours to contact each other and determine an accurate ending date.

The entry of detainer information is voluntary and not required by the TIME System. The alternative to the use of the detainer data is to cancel the warrant record as soon as the entering agency has been advised that the subject is in custody and being held for their agency.

It is not permissible to leave a warrant record in the TIME System without detainer information if the subject has been arrested on the warrant.

- **Caution Indicator**

When an agency lists a subject as a wanted person in the CIB/NCIC databases, they have the option of having their entry bear a notation of 'CAUTION.' This notation should be listed on a warrant/wanted person entry whenever this agency has information that the wanted subject poses a danger to themselves or others. This determination should be made after an examination of all supporting documentation in the case file, to include the original offense the subject is wanted for, past agency dealings with subject, and information listed on criminal history or other files.

- **Vehicle Information**

A vehicle may be entered as part of a wanted person record, provided the location of the vehicle is unknown, and the entering agency has reasonable grounds to believe that the wanted person is operating the vehicle. Mere knowledge or verification with the Department of Transportation that a vehicle is registered to the wanted person does not meet criteria for entry of the vehicle/license plate as part of the wanted person record.

### **Missing Person File**

A record for a missing person who is over the age of 18 may be entered provided this agency possesses signed documentation from a source outside the department supporting the conditions under which the person is declared missing. This written documentation will aid in the protection of the individual's right to privacy. A record for a missing person who is under the age of 18 should be entered within 2 hours of receipt of the minimum data required to enter an NCIC record. Examples are a written statement from a parent/guardian, physician or other authoritative source, statement from a family member, etc. In the absence of documentation from a parent, guardian, next of kin or other authoritative source, including friend or neighbor in unusual

circumstances, or when such documentation is not reasonably available, a signed report by the investigating officer will suffice. Entries into this file are based upon the following categories.

- **Categories**

- ***Disability***

- A person of any age who is missing and under proven physical/mental disability or is senile, thereby subjecting himself or others to personal and immediate danger.

- ***Endangered***

- A person of any age who is missing and in the company of another person under circumstances indicating that his/her physical safety is in danger.

- ***Involuntary***

- A person of any age who is missing under circumstances indicating that the disappearance is not voluntary.

- ***Juvenile***

- A person who is missing and unemancipated under the laws of his/her state of residence.

- ***Disaster/Catastrophe Victim***

- A person of any age who is missing after a manmade or natural disaster/catastrophe, but not confirmed to be dead. Examples include subjects missing after tornado, explosion, possible drowning, etc.

- ***Other***

- A person not meeting entry in any other category and there is a reasonable concern for his/her safety or a person under age 21 and declared emancipated by the laws of his/her state of residence.

- **Missing Person Flags**

- The missing person flag is required for all missing person entries. Many software applications default the standard missing person flag of "MP" behind the scene but allow for modification for the following special circumstances:

- ***Child Abduction Flag***

A child abduction flagging mechanism has been added to missing person entries to facilitate automatic notification to the FBI's National Center for the Analysis of Violent Crimes (NCAVC) and the National Center for Missing and Exploited Children (NCMEC). Use of this automatic alert system may save valuable time in the crucial first 48 hours after a child is abducted.

Upon request, NCAVC provides immediate operational assistance to federal, state, and local law enforcement agencies involved in the investigation of child abduction and serial homicide cases. NCMEC was established to aid the parents of missing and exploited children. It is a national clearinghouse and resource center for missing and exploited children's issues.

The child abduction flag is to be used when the child is under the age of 21, and there is reasonable indication or suspicion that the child has been abducted and/or is missing under circumstances suggesting foul play or a threat to life. Therefore, the Child Abduction Flag can only be used for the missing person categories of Endangered and Involuntary.

The flag is initiated at the local level when an agency enters a child. In order to immediately notify NCAVC and NCMEC, the terminal operator should enter "CA" in the missing person flag field.

For NCIC to work effectively, all entries or records must be packed with as much information as possible. The Remarks Field will assist NCAVC and NCMEC in reviewing cases for immediate attention. Any additional information that will assist law enforcement in identifying special/urgent cases or unusual circumstances should be entered.

The activation of the child abduction flag DOES NOT activate the AMBER Alert System.

- ***Amber Alert Flag***

An Amber Alert capability has been added to missing person entries. Use of the Amber Alert flag will generate an automatic notification to the National Center for Missing and Exploited Children (NCMEC) and the FBI. In addition, NCIC responses will be preceded by a caveat to indicate an Amber Alert was issued.

In order to utilize the Amber Alert flag, agencies must make the determination that an Amber Alert will be issued, following the standard procedures for Amber Alerts. The flag is initiated at the local level when an agency enters a child. The agency must enter an "AA" code in the Missing Person Flag field. Currently no modification of this field is allowed.

Remember that the use of the AA in your missing person entry does not automatically initiate the statewide Amber Alert process and you must still follow the Amber Alert procedures separately.

- ***Disaster Victim Flag***

The missing person flag must be set to "DV" for entry of all missing person disaster victims.

▪ ***Person With Information***

The missing person file allows an agency to add special supplemental information to an already existing missing person record that describes a person who may have information regarding the missing person.

The PWI capability may only be used when:

- The missing person was last seen under circumstances that pose a risk to the safety of that person. Thus PWI information may only be added to missing person records in the endangered or involuntary categories, and only the agency that entered the missing person record may add PWI information to the record.
- There is a substantial likelihood that the PWI has relevant information about the missing person that could result in the recovery of the missing person.
- The identity of the PWI has been disclosed to the general public through an Amber Alert or other formal notification.
- Entering information concerning the PWI could assist the law enforcement agency to identify and interview the PWI and the resulting information could assist in the recovery of the missing person.
- The PWI cannot be located and time is of the essence.
- There is no prohibition under state law on the publication of information concerning the identity of a person for whom a warrant has not been obtained.
- The PWI entry must include agency contact information and guidance for the officer who encounters the PWI.

If the PWI can be entered as wanted (warrant exists, temporary felony want, etc.) the subject should be entered as a wanted person and the records should be linked. Only two PWI may be added to a missing person record, and the PWI information must be reviewed/validated 72 hours after it is entered and every 30 days thereafter.

○ **Caution Indicator**

When an agency lists a subject as a missing person in the CIB/NCIC databases, they have the option of having their entry bear a notation of 'CAUTION.' This notation should be listed on a missing person entry whenever this agency has information that the missing subject poses a danger to themselves or others or the circumstances under which a person has disappeared warrant such a designation. This determination should be made after an examination of all supporting documentation in the case file, to include the case reports, past

agency dealings with subject and/or suspect, and information listed on criminal history or other files.

- **Vehicle Information**

A vehicle may be entered as part of a missing person record, provided the location of the vehicle is unknown, and the entering agency has reasonable grounds to believe that the missing person is operating or is a passenger in the vehicle. Mere knowledge or verification with the Department of Transportation that a vehicle is registered to the missing person does not meet criteria for entry of the vehicle/license plate as part of the wanted person record.

- **National Child Search Assistance Act**

The National Child Search Assistance Act of 1990 requires that agencies verify and update original NCIC missing juvenile entries with any additional information, including medical and dental records, blood type, fingerprint characteristics, jewelry type/description, scars, marks, tattoos and other characteristics fields within 30-60 days of entry.

NCIC will automatically review missing person entries to determine if information is present in the aforementioned fields. If one or more of the fields is missing data, a message (\$K) will be sent via the TIME System to the entering agency. This message should serve as a reminder to make contact with the source of the missing person entry to determine what additional information can be added to the entry. If the entry is updated, the entry will again be searched against other entries.

### **Identity Theft File**

The identity theft file serves as a means for law enforcement to 'flag' stolen identities and identify the imposter when he/she is encountered.

When an individual becomes a victim of identity theft and reports the incident to law enforcement, law enforcement should collect pertinent information from the victim. This information is used to create a victim profile which is entered into the NCIC Identity Theft File. This profile includes information such as victim name, date of birth, social security number and type of identity theft. In addition, the victim chooses a password that will be used to identify that person as the victim in any subsequent police encounters. This password is also entered in the profile listed on NCIC. A caution indicator should be entered when it is appropriate to the particular circumstances of the individual. The reason for the caution must be entered in the Caution and Medical Conditions (CMC) Field.

The Identity Theft File will be searched as part of any NCIC person query. If a match is found, the victim profile will be returned, including password. This provides the officer with the information necessary to verify that the person encountered is the victim or that the person may be using a false identity.

Information on deceased persons may also be entered into the Identity Theft File if it is deemed by the law enforcement agency that the victim's information has been stolen. The record must include the word "DECEASED" in the password field. No consent form is required with the entry of deceased person information.

The victim profile will also include information in the IDT (Identity Theft Type) field about what type of identity theft has been reported:

- ACCT – Checking or savings account
- CFRD – Credit card
- GOVT – Government documents or benefits
- INVT – Securities or other investments
- LOAN – Loans
- NETT – Internet or email
- OTHR – Other
- UTIL – Phone or utilities

○ **Criteria For Entry**

An entry in the Identify Theft File must be supported by an official complaint recorded by a law enforcement agency and obtain a signed waiver form from the complainant. Documentation for the identify theft complaint must meet the following criteria before an entry can be made into the Identity Theft File:

- Someone is using a means of identification of the victim (denoted in the Identity Theft and Assumption Deterrence Act of 1998 as any name or number that may be used alone or in conjunction with any other information to identify a specific individual).
- The identity of the victim is being used without the victim's permission.
- The victim's identity is being used or intended to be used to commit an unlawful activity.

**Unidentified Person File**

The Unidentified Person File is a computerized file that contains records of persons whose identity is unknown. This file is closely associated with the Missing Person File and contains many of the same physical descriptor fields to allow daily, computerized comparisons in an effort to aid in identification. This agency must possess documentation from a source supporting the conditions under which the person/body/body parts have been located. A signed report by the investigating officer will suffice. Entries into this file are based upon the following categories.

○ **Categories**

▪ ***Deceased***

A person who is no longer living for whom the identity cannot be ascertained. This category also includes recovered body parts when a body has been dismembered.

- ***Living***

A person who is living and unable to ascertain his/her identity (e.g., amnesia victim, infant, etc.). The information on unidentified living persons should only be included if the person gives his/her consent or if they are physically or mentally unable to give consent.

- ***Catastrophe Victim***

A person who is a victim of a catastrophe for whom the identity cannot be ascertained or body parts when a body has been dismembered as the result of a catastrophe.

### **Protection Order/Injunction File (POIF)**

Wisconsin statutes require the clerk of circuit court to send a copy of certain orders and injunctions to the sheriff or other appropriate law enforcement agency within one business day of issuance. The clerk is further required to provide information concerning the effective period of the injunction and information necessary to identify the respondent. The law enforcement agency is required to enter the information into the TIME System no later than 24 hours after receiving the information from the clerk. Domestic abuse, child abuse and harassment orders and injunctions are required to be reported. The TIME System will allow, optionally, any other order or injunction to be entered when the information serves a legitimate law enforcement purpose.

Because a restraining order or injunction is issued only after a serious situation has come to the attention of the court, it is important that information on injunctions and restraining orders be entered into the TIME System as soon as possible. Wisconsin and federal law prohibit some persons who are affected by an injunction from possessing a firearm.

The "Ending Date" is a required field for entry of an injunction and the TIME System will not allow the "Ending Date" field to be filled with "NONEXP" for non-expiring. This is done in conjunction with Wisconsin Chapter 813 and the time limits restricted for injunctions. Therefore if your agency receives an injunction with the "Effective Until" or "Ending Date" field not completed it should be returned to the court to obtain the specific date of when the order expires.

Entries into this file are based upon the following categories:

- **Categories**

- ***Domestic Abuse***

Temporary restraining orders or injunctions issued under state statute 813.12. The respondent is prohibited from having firearms under these orders.

- ***Child Abuse***

Temporary restraining orders or injunctions issued under state statute 813.122. The respondent is prohibited from having firearms under these orders.

- ***Harassment***

Temporary restraining orders or injunctions issued under state statute 813.125. The respondent may or may not be prohibited from having firearms under these orders.

- ***Vulnerable Adult***

Temporary restraining orders or injunctions issued under state statute 813.123. "Vulnerable adult" means any person 18 years of age or older who either is a developmentally disabled person or has infirmities of aging, mental illness or other like incapacities and who is substantially mentally incapable of providing for his or her needs for food, shelter, clothing or personal or health care or is unable to report cruel maltreatment without assistance.

- ***Foreign***

Temporary restraining orders or injunctions issued by an out-of-jurisdiction court. The respondent may or may not be prohibited from possessing a firearm under these orders. A foreign protection order shall be accorded full faith and credit by the courts in this state and shall be enforced as if the order were an order of a court of this state if the order meets all of the following conditions: the foreign protection order was obtained after providing the person against whom the protection order was sought a reasonable notice and opportunity to be heard sufficient to protect his or her right to due process and the court that issued the order had jurisdiction over the parties and over the subject matter. A copy of any foreign protection order, or of a modification of a foreign protection order that is on file with the circuit court, that is authenticated in accordance with an act of congress, an Indian tribal legislative body or the statutes of another state may be filed in the office of the clerk of circuit court of any county of this state. The clerk shall treat any foreign protection order or modification so filed in the same manner as a judgment of the circuit court.

- ***Other***

Other types of orders not included in the above categories may be entered. The entering agency must specify the supporting statute that authorizes the issuance of the order.

- **Caution Indicator**

When an agency lists a subject in the CIB/NCIC databases, they have the option of having their entry bear a notation of 'CAUTION.' This notation should be listed on an entry whenever this agency has information that the subject poses a danger to themselves or others or the circumstances under which a person disappeared warrant such a designation. This determination should be made

after an examination of all supporting documentation in the case file, to include the case reports, past agency dealings with subject and/or suspect, and information listed on criminal history or other files.

- **Vehicle Information**

A vehicle may be entered as part of a person record, provided the location of the vehicle is unknown and the entering agency has reasonable grounds to believe that the person is operating or is a passenger in the vehicle. Mere knowledge or verification with the Department of Transportation that a vehicle is registered to the person does not meet criteria for entry of the vehicle/license plate as part of the wanted person record.

### **Violent Gang/Terrorist Organization Files (VGTOF)**

The VGTOF provides law enforcement with identifying information about violent criminal gangs and terrorist organizations and the members of such groups. This information may warn law enforcement officers about the potential danger posed by violent individuals and allow for the exchange of information about these groups and members to aid criminal investigations. The information listed in this file is investigative/intelligence information that has not been subjected to an independent judicial review. Under no circumstances should information from this file be disseminated to non-law enforcement/criminal justice personnel.

- **Group Reference**

Prior to listing a group as a gang or terrorist organization on the TIME System, an agency must possess documentation showing the group meets one of the below definitions. In addition, if the group has not been previously listed on the CIB/NCIC files, an NCIC code must be assigned to the group. This code is obtained by completion and submission of the appropriate forms to NCIC. Forms and further details may be obtained from CIB/NCIC.

- ***Gang***

A gang is an ongoing organization, association or group of three or more persons that have a common interest and/or activity characterized by the commission of or involvement in a pattern of criminal or delinquent conduct.

- ***Terrorist Organization***

A terrorist organization is an ongoing organization, association or group of three or more persons that is engaged in conduct or a pattern of conduct which involves the use of force or violence for the purpose of intimidation/coercion of a government, civilian population or segment thereof to further political or social objectives. Only the FBI may make a terrorist organization entry.

- **Group Member**

Prior to listing an individual as a gang or terrorist organization member on the TIME System, an agency must possess documentation showing the subject meets one of the below definitions.

An individual may be considered a member of a gang or terrorist organization if they have admitted membership in a specific gang or terrorist organization at the time of arrest or incarceration. If the subject does not meet this criterion, they may be considered a member of a gang or terrorist organization if they meet any two of the following criteria:

- They have been identified by an individual of proven reliability as a group member;
- They have been identified by an individual of unknown reliability as a group member and that information has been corroborated in significant respects;
- They have been observed by members of the entering agency to frequent a known group's area, associate with known group members, and/or affect that group's style of dress, hand signals or symbols;
- They have been arrested on more than one occasion with known group members for offenses consistent with group activity;
- They have admitted membership in the identified group at any time other than arrest or incarceration.

- **Caution Indicator**

When an agency lists a subject as a gang or terrorist organization member in the NCIC database, they *do not* have the option of having their entry bear a notation of 'CAUTION.' *All* individual subjects listed as members will have this notation placed on the record.

### **Property Files**

Stolen property may be entered if the owner or custodian of the property has made a theft report. Some property files have special requirements outlined below.

- **Loaned/Rented/Leased Vehicles**

A loaned, rented or leased vehicle or boat that has not been returned may not be entered unless an official police theft report is made or a complaint results in the issuance of a warrant charging embezzlement, theft, etc.

- **Felony Vehicles**

A vehicle used in the commission of a felony or wanted in connection with a felony may be entered immediately providing the whereabouts of the vehicle is unknown. A vehicle does not have to be reported stolen to be listed as a felony vehicle.

- **Stolen/Missing License Plates**

Stolen or missing license plates may be entered into the CIB/NCIC database. If only one license plate was taken the plate may only be entered when the remaining plate is removed/destroyed and the complainant/owner obtains new/corrective registration. If the owner/complainant wishes to retain the same license plate number, no entry can be made to the database. Documentation should be maintained detailing what happened to the remaining plate and the fact that the owner was directed to obtain corrective registration.

- **Recovered Guns**

A gun that has been recovered by this department must be queried through the TIME System to determine if it has been listed as stolen. If not, the gun should be entered as a recovered gun, provided it remains in the custody of this department.

### **Articles Stolen/Lost Articles**

Categories included in this file are: bicycles, camera and photo equipment, data processing equipment, equipment measuring devices and tools, furniture/furnishings, games and gambling apparatus, household appliances and housewares, items of identification, public safety homeland security and critical infrastructure items of identification, special documents/food stamps and tickets, keepsakes and collectibles, livestock, musical equipment, office equipment, personal accessories, radio/TV/sound equipment devices, sports camping exercise and recreational equipment, toxic chemicals, viewing equipment, well drilling equipment and equipment not categorized. This agency will enter stolen and lost articles immediately upon receiving the proper report and documentation.

Public safety, homeland security and critical infrastructure items of identification only such as badges, credentials, police and federal identification cards, military identification, etc., must be entered using an article type code starting with "Q."

- **National Insurance Crime Bureau (NICB)**

The National Insurance Crime Bureau maintains a database of vehicle records. This database includes: Manufacturer's Shipping File, Impound File, Import/Export File, Salvage File, Auction File, Pre-Inspection File, Vehicle Physical Damage Claim File, Rental File, Insurance Theft File, NCIC/CPIC Vehicle Purge Data File, International Index File, Lien Holder File, Mexican OCRA File and EBay Auction File. All NICB entries and queries are based upon a vehicle identification number. Prior to making entries to the NICB impound files, an agency must have the vehicle in question in its possession or control.

- **Caution Indicator**

When an agency lists property in the CIB/NCIC databases, they may have the option of having their entry bear a notation of 'CAUTION.' This notation should be listed on an entry whenever this agency has information that the subjects in a

stolen vehicle/boat are armed and dangerous, or when an agency wishes a recovered stolen item be held for latent fingerprint examination. This determination should be made after an examination of all supporting documentation in the case file, to include the case reports, past agency dealings with subject and/or suspect, and information listed on criminal history or other files.

## **Data Files Modification/Supplementation**

Although data entries may be made with minimum data, it is the policy of this department to enter as much information as is available. If data becomes available at a later date, the record will be modified or supplemented to include the new information. Inquiries should be made to the TIME System DOT files, CHRI files, Department of Natural Resources files, etc., the department's in-house computer system and any other existing records to obtain all the data available. Any new information should be retained with the original case file to show where the identifiers/new information was obtained. Any information that cannot be verified will not be included in the data entry.

## **Data Files Cancellations**

### ***When to Cancel a Data File Entry***

All entries will be removed as soon as it is learned that the person has been apprehended, found, or is no longer wanted, or the property has been recovered. It is not permissible to wait until the person or property is in this department's possession (even if the arresting jurisdiction is holding the person pending outcome of their charges). The entry must be cancelled as soon as practicable. The only exception to this section is if the CIB wanted person detainer function is utilized. Details of the detainer function may be found in the section of this policy dealing with entry of wanted person records. Once a record has been cancelled, documentation of the cancellation and reason for cancellation will be retained in the case file. The record should be queried again to ensure that it has indeed been removed from the database.

### ***Purged Records***

Records entered to the CIB/NCIC databases are retained in these files for a specified period of time. When the specified time period has passed, records are purged from the databases. When notice is received a record has been removed from the database the case file will be annotated to reflect this. These records will not normally be re-entered unless there is some investigative value to re-entering the item to extend the retention period. This determination will be made on a case by case basis. Retention periods for the various files are outlined below.

### **Warrant/Wanted**

Warrants remain on file indefinitely, or until the entering agency cancels the entry.

- **Temporary Felony Want**

Remain on file 48 hours.

- **Temporary Misdemeanor Want**

Remain on file 72 hours.

- **Detainer Information**

Warrants with detainer information appended will remain on file until the date sentence ends specified by the entering agency. When purged, the warrant record itself, along with detainer information, is removed from the file.

### **Missing Persons**

Missing person entries remain on file indefinitely or until the entering agency cancels the entry.

### **Identity Theft**

Identity theft entries remain on file until the entering agency cancels it or until the Date of Purge (DOP) is equal to the current date. The maximum retention period for an identity theft record is 5 years.

### **Protection Orders/Injunctions**

Protection order/injunction file entries remain on file until the specified date of expiration.

- **Temporary Restraining Orders**

Remain on file for 96 hours after the specified expiration date of the order.

### **Violent Gang/Terrorist Organization**

- **Organization**

Organization entries remain on file indefinitely, or until the entering agency cancels the entry.

- **Member**

VGTOF member entries remain on file for five years, or are purged on an earlier date specified by the entering agency.

### **Unidentified Persons**

Unidentified person entries remain on file indefinitely, or until the entering agency cancels the entry.

## **Vehicles**

- **Stolen Vehicles**

If a vehicle identification number or owner applied number is included in the entry, stolen vehicle entries remain on file for four years plus the remainder of the year of entry. If one of the two identifying numbers is not included the record will be purged after ninety days.

- **Felony Vehicles**

Remain on file ninety days.

- **Stolen/Missing License Plates**

Remain on file for four years plus the remainder of the year of entry.

## **Parts**

Remain on file for four years plus the remainder of the year of entry.

## **Articles**

Remain on file for one year plus the remainder of the year of entry with the exception of articles entered with a Type Code starting with "T" or "Q" which remain until the entering agency cancels the entry.

## **Guns**

Stolen and lost gun entries remain on file indefinitely, or until the entering agency cancels the entry. Recovered gun entries remain for two years plus the remainder of the year of entry.

## **Boats**

If a boat hull number or owner applied number is included in the entry, stolen boat entries remain on file for four years plus the remainder of the year of entry. If one of the two identifying numbers is not included the record will be purged after ninety days.

## **Securities**

Remain on file for four years plus the remainder of the year of entry.

- **Traveler's Checks and Money Orders**

Remain on file for two years plus the remainder of the year of entry.

## **Validation**

Validation obliges the entering agency to confirm the record is complete, accurate and still outstanding or active. Validation is accomplished by reviewing the original entry and current supporting documents. Recent consultation with any appropriate complainant, victim, prosecutor, court, motor vehicle registry files, or other appropriate source or individual also is. In the event the ORI is unsuccessful in its attempts to contact the victim, complainant, etc., the entering authority must make a determination based on the best information and knowledge available whether or not to retain the original entry in the file.

### ***Validation Officer***

This department will designate a validation officer. This person will attend CIB Validation/Quality Control training.

### ***Validation Schedule***

Records for validation are selected from the CIB/NCIC databases based upon the month of entry as outlined below. A listing of records requiring validation is then forwarded to this department, along with a certification letter.

#### **January**

January validation includes records entered in October.

#### **February**

February validation includes records entered in November.

#### **March**

March validation includes records entered in December.

#### **April**

April validation includes records entered in January.

#### **May**

May validation includes records entered in February.

#### **June**

June validation includes records entered in March.

#### **July**

July validation includes records entered in April.

#### **August**

August validation includes records entered in May.

**September**

September validation includes records entered in June.

**October**

October validation includes records entered in July.

**November**

November validation includes records entered in August.

**December**

December validation includes records entered in September.

***Accuracy of Records***

The accuracy of records is an integral part of the system. The verification of a record should include assuring all available crosschecking was made and that the data in the record matches the data in the investigative report.

Maintaining accurate files means more apprehensions and recoveries will be made.

It is the duty of the validation officers to ensure the accuracy of the entries into the CIB/NCIC files. During validation, an examination will be conducted of each record, comparing the entry to the supporting documentation to ensure the entry accurately reflects the information available to the department.

***Completeness of Records***

Complete records include all information that was available on the person or property at the time of entry. The validation process should include a review of whether additional information has become available (missing from the original entry) that could be added. This is accomplished by conducting queries on the person/item through all available databases/information sources (i.e., DOT, CHRI, DNR, departmental records, etc.) and reviewing responses to obtain new or additional information. Stale information will be removed and updated information added. All changes will be documented.

Complete inquiries on persons include numbers that could be indexed in the record; i.e., Social Security, Passport, VIN, License Plates, Driver's License, etc. Inquiries should be made on all names/aliases used by the suspect. Complete vehicle queries include VIN and License Plate Numbers.

***Validity of Records***

No records entered by this department into the CIB/NCIC files will be retained on such files without verification from the person or office/official responsible for the initial report, or from someone who has assumed responsibility for the record/property (i.e., an insurance

company). An entry may remain in the CIB/NCIC database without such verification if this department determines there is some investigative value in maintaining the entry.

During the validation process this department will make contact with the originating party of each record, either by personal contact, letter/memo, or telephone. Contact will be made with the clerk of court and/or district attorney to determine if a warrant is still outstanding.

### **National Child Search Assistance Act**

The National Child Search Assistance Act of 1990 requires that agencies verify and update original NCIC missing juvenile entries with any additional information, including medical and dental records, blood type, fingerprint characteristics. Jewelry type/description, scars, marks tattoos and other characteristics fields within 30-60 days of entry.

NCIC will automatically review missing person entries to determine if information is present in the aforementioned fields. If one or more of the fields is missing data, a message (\$K) will be sent via the TIME System to the entering agency. This message should serve as a reminder to make contact with the source of the missing person entry to determine what additional information can be added to the entry. If the entry is updated, the entry will again be searched against other entries. During validation this department will ensure follow-up is conducted on missing person reports to determine if the subject is still missing and attempt to obtain any missing information that would assist in identifying the missing person if found.

### **License Plates**

Vehicle license plates will only be retained in the database if a check of registration status indicates the plate was cancelled or otherwise not currently in use. If a registration check shows current registration, the entry will be cancelled.

### ***Certification***

Records for validation are selected from the CIB/NCIC databases based upon the month of entry. A listing of records requiring validation is available to the department online via the eTIME Browser. The agency must certify that the validation is complete. Due to the limited time which the CIB has to validate these files with NCIC, IF THE CERTIFICATION IS NOT RECEIVED BY THE DATE INDICATED, CIB HAS NO ALTERNATIVE BUT TO PURGE ALL OF THE RECORDS FOR THAT MONTH. Certification acknowledges that all inactive records have been cancelled; all incorrect records have been modified; and presently all records on the computerized data files entered by this agency are correct and accurate. The validation officer is responsible for ensuring validation is completed within the applicable period and that CIB is notified of certification by the specified due date.

### ***Advisory Messages***

All quality control and other advisory (\$) messages shall be reviewed by a validation officer in a timely fashion. These messages include, but are not limited to, the following.

**File-Transfer-Ready Notification (\$B)**

A \$B administrative message is transmitted to an ORI whenever a file is available for retrieval. This situation occurs when: 1) Excessive hits resulting from an inquiry is transmitted. 2) A response to a batch inquiry is transmitted.

**Duplicate Vehicle (\$D)**

When a vehicle locate, clear, or cancel transaction is processed by NCIC and there are duplicate records on file (VIN and VMA or LIC, LIS, LIT and LIY exactly match), a message is sent to the owner(s) of the duplicate record(s). If such a message is received, the terminal operator will query the possible duplicate record and forward the message and a copy of the possible duplicate record to the investigating officer for the case.

**Quality Control Notice/Serious Error (\$E)**

When errors are identified in entries to the CIB/NCIC files, the entering agency is advised of the error through receipt of a \$E Serious Error Notification from NCIC or a Quality Control Notice from CIB. Both advise of a significant error in a specific entry. NCIC Serious Error Notifications indicate the erroneous record has been removed from the file, whereas a CIB Quality Control Notice generally advises the agency of the error and provides a deadline for correcting it. The receipt of such a message by this department will cause the error to be corrected and the record to be re-entered, as necessary. If correct information is not readily located in the case file, the case will be forwarded to a supervisor to be assigned to a department member for follow-up investigation to attempt to locate correct information for entry to the database.

**Gang (\$G)**

When an originating agency no longer has an interest in a violent gang/terrorist organization record or the record (interest) has been entered in error, the originating agency may cancel the record. If the "oldest" agency (primary ORI) cancels the record, that agency's ORI and POC are removed. If there are no other agencies associated to the record, the entire record is cancelled. If there are other agencies associated to the record, ownership of the record is transferred to the next "oldest" agency which then becomes the primary ORI. Cancellation by any agency other than the primary ORI simply removes that agency's ORI and POC from the record. If a message is received advising that this agency is now the primary ORI responsible for a gang/terrorist organization record it will be forwarded to a supervisor.

**Delayed Hit (\$H)**

A message is sent to the ORI entering or modifying a record which resulted in a hit response for an inquiry made within the last 5 days. A message is also sent to the ORI of an inquiry transaction when a hit response is generated because of a subsequent entry or modification transaction. The inquiring agency will potentially receive hit responses for 5 days after the initial inquiry was made. A \$.H. administrative message will not be sent to an agency that hits on a delayed queue inquiry which has the U. S. Customs Service's ORI VAUSC6099 unless the entry or modification transaction is to the Violent Gang and Terrorist Organization File or the Deported Felon File.

Upon receipt of a delayed hit message indicating this department was the inquiring agency, the validation officer will make a reasonable effort to ascertain what terminal/officer initiated the query. The validation officer will also query the possibly wanted subject/vehicle to attempt to ascertain if the subject/vehicle is still wanted. If the entry is still active, and the validation officer is able to ascertain who initiated the query, the validation officer will advise a supervisor of the information. The information will then be forwarded to the initial inquiring officer and/or presented to all staff in an attempt to locate the subject/vehicle.

#### **Originating Agency Notification (\$H)**

A message is sent to the ORI of record when an inquiry, enter, or modify transaction results in a hit response and the Notify Originating Agency flag (NOA) is set to Y in a NCIC 2000 formatted record.

#### **Investigative Interest (\$I)**

NCIC has developed a concept to create a supplemental entry that allows agencies to indicate an investigative interest on another law enforcement agency's NCIC record entry. This concept pertains to any type of record entry that is currently listed in the NCIC files. If an agency receives a record response to an NCIC query containing investigative interest information, the inquiring agency is not required to notify the investigative interest agency(s), but it is recommended that they do so. Multiple agencies can append their interest to an NCIC base record. A \$I Investigative Interest Notification is sent to the ORI of the record when an investigative interest supplement record is entered or cancelled.

#### **Emancipated Juvenile (\$J)**

This message is sent to the ORI of a wanted juvenile record when the individual of the record reaches the age of emancipation. The message may be generated by NCIC or CIB. Upon receipt of this message the validation officer will make contact with the city attorney, district attorney, or court to ascertain whether the warrant should remain on the system, be cancelled, or be reissued charging the subject as an adult.

#### **Incomplete Missing Person (\$K)**

NCIC will automatically review missing person entries to determine if information is present in the aforementioned fields. If one or more of the fields is missing data, a message (\$K) will be sent via the TIME System to the entering agency. This message should serve as a reminder to make contact with the source of the missing person entry to determine what additional information can be added to the entry. If the entry is updated, the entry will again be searched against other entries. Upon receipt of a \$K message, it will be forwarded to the investigating officer of the case, along with a request he/she attempt to obtain the missing information and forward it to the appropriate personnel for entry into the system.

#### **Locate (\$L)**

The purpose of a locate message is to indicate (until the originating agency cancels the record) that the wanted person has been apprehended or stolen property has been located. If the ORI fails to cancel the NCIC record, the Locate will purge it within two weeks of placement. In the missing person file, a locate message indicates the whereabouts of the missing person has been determined and immediately purges the record from the file. If a CIB record is being located, TSCC will contact the ORI and explain why the locate is being placed against the record. TSCC will advise the ORI that they have approximately **TWO** hours to cancel the record. If the ORI fails to cancel the record within the time allotted, TSCC will cancel the record. This message is placed against a record that remains active in the system after hit confirmation has taken place. The locate message includes the date and time the person or property was located, as well as the name of the locating agency. If a record of this department is subject to a locate, the record will be immediately fixed or cancelled, as appropriate.

### **Possible Match (\$M)**

A message is sent to the ORI initiating an entry/modification transaction that results in potentially positive hits during a comparison of the missing/unidentified person files. It is also sent to the ORI(s) of record for the possible matches from the comparison. Upon receipt of such a message, the inquiring agency must review all of the information in the candidate record(s) and contact the agency(s) that entered the record(s) to confirm possible matches.

If a possible match message is received regarding one of the department's records the investigating officer of the case will be notified as soon as practicable. In addition, the terminal operator will query the possible matching record in the system to receive a complete printout. The terminal operator will also make contact with the entering agency of the possible matching record, either by telephone or via administrative message, advising them of the receipt of the possible match notice and to obtain contact information for the investigating officer responsible for the possible matching record. All information obtained will be forwarded to the investigating officer.

### **No Match (\$N)**

A message is sent to the ORI initiating an entry/modification transaction that results in no potential matches during the missing/unidentified person comparison. If such a message is received it will be retained in the case file and the investigating officer notified.

### **Incarcerating Agency (\$O)**

NCIC has created the ability for law enforcement agencies to enter detainer information to an NCIC wanted person record, after a positive hit confirmation response has been received. In Wisconsin there is no ability for an agency to enter this data. However, a detainer in NCIC may generate a \$O Incarcerating Agency Notification to a Wisconsin agency. This message provides formal notification via the TIME System that an NCIC detainer has been filed. This message will be forwarded to appropriate personnel and retained in the detained subject's file to ensure staff is aware of the fact another agency wishes to take custody of the subject.

### **Purge (\$P)**

This message is sent to the entering agency when a record has been retired because it has reached the end of its retention period. This message may be generated by NCIC or by CIB, and may be sent to the entering agency via the TIME System or US Mail. Upon receipt of the annual purge listing of articles, vehicles and parts, the case file should be annotated to show that the record has been purged from the computer files.

### **Hits to Wants**

When a wanted person file entry contains an FBI number, the same wanted information is posted in the subject's FBI III criminal history record. If the FBI receives subsequent arrest fingerprints that are identified with the criminal history record, the NCIC System sends an automatic notification message, referred to as a hits-to-wants message, to the wanting agency to inform them that the wanted person has been arrested. The validation officer should investigate to determine if the wanted subject remains in custody of the agency submitting fingerprints, or if not, attempt to obtain from that agency further descriptive and location information for the subject which may be included in the TIME System entry or used for apprehension of the wanted person.

### **Hot Check Initiative**

The FBI has implemented a hot check initiative. The hot check initiative is the automatic name based search of specific NCIC files that will occur for all Integrated Automated Fingerprint Identification System (IAFIS) ten print submissions. For each IAFIS criminal and civil applicant ten-print submission, the interstate identification database will send one inquiry request to NCIC, searching the Wanted Person File and the Violent Gang and Terrorist Organization File. After the search is completed, the following notification of the hot check inquiry will be generated and sent to the agency(s) that entered the NCIC record(s) as an administrative message. If the agency that entered the NCIC record determines that the subject of the ten-print submission is potentially the subject of the NCIC record, then the entering agency should contact the contributing agency as necessary.

### **Detainer**

The detainer file allows an agency warrant/wanted person record to remain entered after hit confirmation has occurred, but the arrested subject will not be released to the agency holding the warrant. Detainer information is appended to the already existing warrant/wanted person record and can only be placed on a record that has a locate placed on it. This information may include details of where the subject is being held, how long he will be held, and miscellaneous remarks. There will be times when the conditions of the sentence will change and/or multiple agencies will have warrants for the same subject. When this occurs, the detainer must be modified with each change of sentence and/or place of incarceration. If detainer information is appended to a record, the agency must maintain documentation of the information listed in the detainer.

The ending date must be a documented date accurately representing the anticipated transfer of the subject by the incarcerating agency to your department. The requirement of the ending date field as mandatory was designed to automatically clear old records by purging them after this date. If a record containing detainer information is audited during a biennial audit and found to contain an undocumented or inaccurate ending date it will be counted as wrong the same as any other record containing fictitious/undocumented data.

If the subject is not immediately available for pick up and the agency is unable to determine the ending date at the time of entering the detainer information, a date of 10 days or less may be entered as the ending date. This will then generate the automatic messages to both the incarcerating agency and the entering agency at approximately 0000 hours of the ending date. This allows the incarcerating and entering agency 24 hours to contact each other and determine an accurate ending date.

The entry of detainer information is voluntary and not required by the TIME System. The alternative to the use of the detainer data is to cancel the warrant record as soon as the entering agency has been advised that the subject is in custody and being held for their agency.

It is not permissible to leave a warrant record in the TIME System without detainer information if the subject has been arrested on the warrant.

### **Juvenile Missing Person Emancipation**

If an individual has been entered as a missing person juvenile and the record is still outstanding when the individual turns 18, a message will be sent to the ORI of the record from the Wisconsin Crime Information Bureau.

## **Administrative Messages**

An administrative message is a point-to-point free form message. This criminal justice related message may be asking for information or assistance, or it may be in response to a request from another agency. It is differentiated from other messages in that it is free form and may be used for practically any type of information transmission not associated with a specific message type. If the administrative message includes information that is related to officer safety (i.e., armed and dangerous), this phrase should be placed at the front of the message on its own line to highlight it. Administrative messages may be routed terminal to terminal, terminal to multiple terminals, or terminal to area.

### ***Prohibited Administrative Messages***

To ensure the system remains dedicated to transmitting essential law enforcement/criminal justice information, the following types of administrative messages are **PROHIBITED**:

- Announcements of social affairs, retirement parties, labor-management affairs and seasonal goodwill messages such as Christmas/New Year's greetings.
- Messages supportive of or in opposition to political issues, including announcements of meetings relating to such issues.
- Messages supportive of or in opposition to labor-management issues, including announcements of meetings relating to the same.
- Messages supportive of or in opposition to legislative bills.
- Messages related to the advertising of equipment for sale.
- No recruitment of personnel (job opening/interviews).
- No excessively long messages.

- No messages relating to requests for information concerning salary, uniforms, personnel, or related items that can be routinely obtained by correspondence or means other than the TIME System.
- No messages regarding wanted subjects or vehicles if they can be entered into NCIC.
- No solicitation of funds.
- No NLETS training messages that include the name of a company that is providing the training unless the company is not-for-profit and is providing a direct service. Training announcements may be sent via Regional broadcast codes to states in geographic proximity of the sender only.
- Messages not relating to official or authorized business.

### ***All Points Broadcasts (APBDs)***

The restrictions listed have been adopted for APBDs (sometimes referred to as state-wide broadcasts). Recognizing that there may be circumstances where the seriousness of the situation overrides the normal policy prohibitions, the restrictions may be waived under the following conditions:

- A user has information that is pertinent to a criminal investigation that is of interest to all states and cannot be entered into NCIC.
- A user has information regarding kidnapping, skyjacking or other serious criminal acts. Keep messages as brief as possible.
- A user has information on a wanted person that cannot be entered into NCIC but is of interest to all states.

If there is information in the APBD request that qualifies for entry into any of the data files, the APBD will not be approved until the applicable data has been entered into CIB/NCIC.

All requests for nationwide or statewide APBDs MUST be directed to the TIME System Control Center (TSCC) and must be of significant importance to law enforcement. If your agency needs to request a broadcast in a specific state, send a message to that state's control terminal. An attempt to locate in Canada or a Canada-wide broadcast request must be sent to INTERPOL in Washington, D.C. (DCINTER00). If an out-of-state agency contacts your agency requesting a broadcast, refer them to TSCC.

The following APBD regulations will be used to evaluate requests for all points broadcasts. Requests for APBDs (state and/or nationwide) will be approved if the message falls within one of the following categories:

#### **Death/Aggravated Battery to Law Enforcement w/Suspect at Large**

Adequate physical description of suspect and/or vehicle is required. "Adequate" means enough information to recognize the person or vehicle if seen.

#### **Felonies Involving Armed/Believed to be Armed Fugitive(s)**

Adequate physical description of the fugitive and/or vehicle is required.

#### **Escapees From Custody**

This includes all escapees from: officer custody, city and county jails, prisons, detention homes/centers, work camps and juvenile facilities.

### **Death Notices of Actively/Formerly Employed Law Enforcement Officials**

In-state APBDs may also include public safety officials.

### **Attempts to Locate (ATLs)**

When foul play is suspected or known and is so specified. Adequate physical description of the person and/or vehicle is required. For death or serious illness message delivery only if the direction of travel is unknown. If the direction of travel is known, the requesting agency must send messages to the specific agencies along the route of travel (an AREA/HIGHWAY broadcast may be used under appropriate circumstances).

### **Found Unidentified Bodies or Body Parts**

### **Information That Has State/Nationwide Law Enforcement Significance**

This may be a description of the method of operation (M.O) requesting information from similar cases or alerting other agencies of same, or a request for information on a person in custody refusing to cooperate by not giving name, etc. The requesting agency can ask for assistance based on the description of the person and circumstances surrounding the case. If the request concerns stolen property that cannot be entered into CIB/NCIC, the list of property items must have state or nationwide significance and be condensed into no more than 15 lines of text. Give general descriptions without listing all of the quantities. Any information that cannot be entered into CIB/NCIC that is pertinent to a criminal investigation and would be of interest to state or nationwide law enforcement agencies.

### ***Area/Highway/Transport Broadcasts***

The same categories and rules are to be used when considering an **AREA / HIGHWAY / TRANSPORT** broadcast; the difference being that the information in the message pertains to a specific area of the state rather than having state or nationwide significance. The area broadcast can be sent by an individual agency, it is not to be requested through TSCC.

### ***Training Broadcasts***

All announcements of **training** being hosted or sponsored by the originating agency must be sent to the broadcast area "TRNG". An agency may transmit up to three training announcements for each training session to be held. The receipt of "TRNG" training broadcasts is entirely voluntary. Your TIME Agency Coordinator (TAC) can request to have terminals added or removed from the "TRNG" broadcast group. Agencies utilizing training broadcasts should closely monitor its use and compliance with this new policy in an effort to make the most efficient use of this valuable resource.

### ***Urgent Message Indicator***

Designating a message as 'urgent' will cause an audible noise to be played when the message is received at another terminal. In addition, there will be a visual notification/pop-up displayed on the receiving terminal indicating an urgent message has arrived.

This department will utilize the urgent function to avoid missing important messages. Only the administrator will have the authority to disable the function and/or change the sound of the .wav file.

Employees of this department will consider all outgoing messages as urgent and will send them with the urgent function activated by typing URGENT as the first item in the reference line.

## **Hit Confirmation**

A TIME System hit will generally provide reasonable suspicion for a stop so long as the information given resulting in the hit was reasonably accurate (i.e., the officer read the license plate or serial number correctly). When an officer checks with the dispatcher to evaluate all available descriptors from the hit against the person/property stopped and it appears reasonable that there is a potential match, the officer may detain the person/property for a reasonable amount of time while hit confirmation takes place. A TIME System hit may not, in and of itself, be probable cause to arrest a person or seize property. It is one fact that must be added by the officer in arriving at sufficient legal grounds for arrest or seizure of property. The older the hit entry and the less descriptive the information available, the more independent facts the officer must develop to establish probable cause. To aid in the officer's decision, hit confirmation must take place prior to making an arrest/seizing property.

Confirming a hit means to contact the agency that entered the record to ensure that the person or property inquired upon is identical to the person or property identified in the record, ensure that the warrant, missing person report, protection order or theft report is still outstanding, and obtain a decision regarding the extradition of a wanted person when applicable, information regarding the return of the missing person to the appropriate authorities, information on the conditions of a protection order or information regarding the return of stolen property to its rightful owner.

### ***Hit Confirmation Levels***

There are two levels of priority when requesting to respond to a hit confirmation.

#### **Urgent**

An agency must respond to the requesting agency within ten minutes advising either the status of the validity of the entry and other information pertaining to the case or advising the amount of time it will take to respond to the request with the needed information. This priority should be used where the hit is the only basis for detaining a suspect, or the nature of the case requires urgent confirmation.

#### **Routine**

An agency must respond to the requesting agency within one hour advising either the status of the validity of the entry and other information pertaining to the case or advising the amount of time it will take to respond to the request with the needed information. Generally this is used when the person or property is being held on local charges and urgent confirmation is not needed.

## ***Hit Confirmation Request Steps***

### **Check the computer results with the original query**

Compare the hit received with the original information queried upon. Ensure you are within any geographic restrictions listed on warrant entry. Ensure subject or item is in custody. No hit confirmation message should be sent when a record contains a geographic/extradition limitation and the person is outside the restriction indicated. An administrative message may be sent to the entering agency to advise them of the location of the person as an investigative update/courtesy, but be sure to indicate the subject is not being held due to the restriction on the record.

### **Check with the requesting person for additional information**

Additional information may clarify the hit. Relay to the requesting person all identifying information such as height, weight, hair color, eye color, scars/marks/tattoos, etc.

### **Check with the ORI to verify the record**

When it is believed to be a valid hit and the department is able to arrest the wanted person or recover the stolen property, confirm with the entering ORI that the entry is valid, and obtain any further identifying information or information about the case that would be useful to the investigating officer. Send the appropriate TIME System message requesting confirmation. Hit confirmation should be done using the appropriately formatted screens. Hit confirmation may *not* be done using administrative message formats. If no response is received within the designated time period, a second request may be sent. A follow-up phone call to the entering agency is recommended.

### **Obtain hard copy documentation**

Obtain hard copy documentation from the entering ORI on the results of the hit confirmation request and disposition of the person/item. This provides proof of the information that was used to make the decision to arrest/seize property.

### **Query all identifiable data not queried originally**

Additional identifiers may be discovered during the hit confirmation/arrest process. Querying these identifiers may result in other hits being discovered for the person/property.

## ***Hit Confirmation Responses***

If an agency maintains entries into the data files of CIB/NCIC they are required to ensure hit confirmation is available 24 hours a day. When a request for hit confirmation is received this department will respond within the specified time period. Remember, this response does not necessarily need to confirm the hit, but must at least acknowledge the hit request and provide an approximation of the amount of time it will take to confirm the hit. The operator receiving the hit request should retrieve the case file involved and check the file to ensure the entry is valid. The operator should make sure the requesting agency is within any geographic/extradition restrictions specified. If the entry is valid and the requesting agency is within the specified limits, the operator should advise the requesting agency of the validity

of the hit and request information of the holding agency as to the disposal/retrieval of the person/property. Once the hit has been confirmed and the requesting agency advises they have the person/property in custody, the original entry should be cancelled. It is not permissible to wait until the person or property is in this agency's custody before canceling the record. The only exception to this process would be the use of the detainer in regards to the wanted person file.