# TIME System Newsletter
Volume   2013-1
March 2013

Did you know that the TIME System is over 40 years old? The TIME System went live in October 1972 as a result of a project initiated in 1971. The original project was called "WATCH" (Wisconsin Access to Criminal History). The project was renamed to "TIME" (Transaction Information for the Management of Enforcement) during the development process, a name that remains today and is defined within Wisconsin statutes. The TIME System Control Center (TSCC) was created to oversee the daily program operations of the TIME System ensuring maximum uptime and responding to user inquires. In 1981 oversight of TSCC was moved from the Crime Information Bureau (CIB) to the Bureau of Computing Services (BCS) within the Department of Justice. Effective April 1, 2013, oversight of TSCC will return to CIB. Most of you probably thought TSCC has always been part of CIB due to its close connection to the TIME System. This transition from BCS back to CIB will go unnoticed to you but I wanted to make you aware of this change. As always, we will continue to provide you with the best service possible and are always open to any suggestions you may have that will help us to improve.
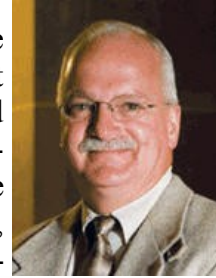
The TIME System processed 49,704,816 transactions in 2012 for a daily average of 136,178. The TIME System peak processing times remain 4-6 pm and the slowest times 4-6 am daily. Not at all surprising, person and vehicle inquires represent 42% and 41% respectively of the total TIME System transactions in 2012. This is consistent with national statistics that show vehicle and person inquiries being the #1 and #2 transactions processed by Nlets (The International Justice & Public Safety Network). Wisconsin is not among the top 3 states accessing Nlets (Texas, California and Michigan) but still contributes a significant number. Nlets processed 1,333,721,297 transactions in 2012. That is not a typo, Nlets processed over 1.3 billion transactions in 2012. Wisconsin represents approximately 1 million of those transactions per month.

The 2013 CIB Conference is scheduled for September 11th – 13th in Green Bay. More information related to the conference is included in this newsletter including a credit card payment option for the registration fees. Hope to see you there.

Please feel free to contact me or any of the CIB staff to discuss your thoughts on how we can continue to improve.

Walt Neverman

Director CIB

Background Checks

You sent in the fingerprint card on your new employee to complete the required fingerprint based background check. How do you know the fingerprint card was received by CIB and processed? How do you know what the results of the background check were? Does your new employee have a criminal history that would disqualify them from accessing the TIME System?

The results of applicant fingerprint based background checks are posted to CIB's online record check system. It is the responsibility of the submitting agency to go to the website and retrieve the results of the background check within 30 days. Agencies should routinely check the website http://wi-recordcheck.org for background check results. Navigate to the "Background Checks for Account Customers" section of the site, enter your agency's account number and PIN and click on the button for "Previous Orders".

Remember, if a felony conviction of any kind exists, the agency must deny the person access to the system. The agency may ask for a review by CIB in extenuating circumstances where the severity of the offense and the time that has passed would support a possible variance. If a record of any other kind exists, the agency must review the matter to determine if access to the system is appropriate.

Further information about accessing the online record check system and background check results can be obtained from CIB's Record Check Unit at 608-266-9398.

Remember, HELP is Available

Ever read a response from the TIME/NCIC/Nlets Systems and been confused? What does that abbreviation mean? Is a class D driver's license the same everywhere? Can I get concealed carry information from Georgia?

System users should keep in mind that the TIME/NCIC/Nlets Systems have help files built in. Users can find answers to questions, like those above, by simply accessing the appropriate HELP File. The HELP Files are computerized informational messages prepared and updated by each state and housed at Nlets. They advise the fields and codes required to access records in the different files, as well as provide an explanation and sample of how the files work and the output received.

There are multiple HELP Files that can be accessed, including driver's license information, vehicle registration information, boat and snowmobile information, criminal history record information, information on states providing automated criminal history, information for officers flying armed, Nlets license plate recognition information, information on states providing automated road/weather information, concealed carry information and state wanted query information. Help for Canadian provinces is also available.

Portal 100 users can find the needed HELP Files transaction in the Nlets/NCIC Special Messages section of the menu, transaction #0496.

DNR Changes

The Wisconsin Department of Natural Resources implemented changes to their system that affect TIME System users.

Person Queries: Search criteria for DNR person queries have changed. Responses will only be returned if an exact match of the queried information is found. The wildcard character (%) is now only allowed in the last and/or first name field (at the end) when querying DNR person files using transaction #0961. The wildcard character can no longer be used when querying DNR files by number. Multiple responses to a query may be returned, depending on the query information matched. For example, a query by name, DOB and social security number may return a response matching the name and date of birth and another response matching the social security number queried. These responses may or may not be duplicates.

Two DNR files are checked when DNR person queries are made: the customer file and the citation file. The customer file contains information on DNR licenses, permits, etc. issued to a person, along with boats, snowmobiles and ATVs that may be registered to that customer. The citation file contains information on citations issued for violations of DNR rules/statutes and now includes citations issued from 1987 to present date. The two files are searched independently; you may receive responses from one or both files and citation information may be duplicated. In addition, responses may be received from the citation file for persons who have received a citation, but do not have a DNR customer number or license.

Vehicle Queries: The updates to the DNR system have affected DNR vehicle registration queries as well. An ATV or snowmobile registration query will only generate a DNR response when the user queries the registration number or vehicle identification number. The registration number should be queried without the two letter prefix of AT or SN. A query of a machine's decal number, if different from the registration number, will now generate a 'NO RECORDS FOUND' response.

This change creates an issue with older private and/or agricultural registered ATVs. When making a stolen vehicle entry, if the decal number of the ATV/snowmobile (which should be attached to the machine) is different than the registration number, enter the decal number in the Owner Applied Number field.

Wisconsin boat registration queries by registration number are still required to include the two letter prefix code of WS, as this prefix does appear on the boat and is considered part of the registration number.

Questions on the new search criteria and responses returned should be directed to the DNR at 1-888-936-7463.
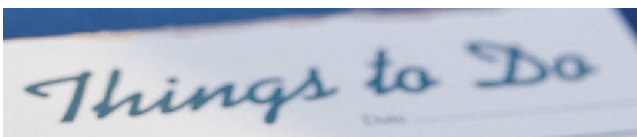
Check Your List

TIME System agencies are reminded that CJIS Security Policy 5.5.1 requires that each agency validate their list of TIME/NCIC system accounts at least annually and document the validation process. Has your agency completed its annual review of system accounts/logins?

Juvenile Fingerprints

Law enforcement agencies are aware that they must obtain and submit to CIB finger-prints for adults arrested or charged with certain offenses. Not every agency is clear, however, on whether fingerprinting of juveniles is required, or even allowed. The state laws that govern fingerprinting are in Chapter 165 of the Wis. Stats. First, s. 165.84(1) indicates that law enforcement agencies must take fingerprints and forward them to DOJ:

165.84 Cooperation in criminal identification, records and statistics
(1) All persons in charge of law enforcement and tribal law enforcement agencies shall obtain, or cause to be obtained, the fingerprints in duplicate, according to the fingerprint system of identification established by the director of the F.B.I., full face, profile and full length photographs, and other available identifying data, of each person arrested or taken into custody for an offense of a type designated in s. 165.83(2)(a).

Then s.165.83(2)(a)(1-5) specifies what offenses fingerprints must be taken for:
165.83 Criminal identification, records and statistics
(2) The department shall:
(a) Obtain and file fingerprints, descriptions, photographs and any other available identifying data on persons who have been arrested or taken into custody in this state:
1. For an offense which is a felony or which would be a felony if committed by an adult.
2. For an offense which is a misdemeanor, which would be a misdemeanor if committed by an adult or which is a violation of an ordinance, and the offense involves burglary tools, commercial gambling, dealing in gambling devices, contributing to the delinquency of a child, dealing in stolen property, controlled substances or controlled substance analogs under ch. 961, firearms, dangerous weapons, explosives, pandering, prostitution, sex offenses where children are victims, or worthless checks.
3. For an offense charged or alleged as disorderly conduct but which relates to an act connected with one or more of the offenses under subd. 2.
4. As a fugitive from justice.
5. For any other offense designated by the attorney general.

Finally s. 165.83(1)(c) specifies that this requirement includes those age 10-17:
(1) Definitions. As used in this section and s. 165.84:
(c) "Offense" means any of the following:
1. An act that is committed by a person who has attained the age of 17 and that is a felony or a misdemeanor.
2. An act that is committed by a person who has attained the age of 10 but who has not attained the age of 17 and that would be a felony or misdemeanor if committed by an adult.
3. An act that is committed by any person and that is a violation of a city, county, village or town ordinance.

In addition, the issue was addressed in an attorney general's opinion:
62 Atty. Gen. 45.
Pursuant to sub. (2), identification records should be made by local law enforcement agencies of juveniles arrested or taken into custody for confidential reporting to the department of justice.

Wisconsin Department of Justice

2013 CIB CONFERENCE
START PLANNING NOW

Wednesday September 11th – Friday September 13th, 2013
Radisson Hotel & Conference Center, Green Bay

This year's conference offers sessions of interest to Patrol Officers, Investigators, Administrators, IT, Dispatchers, District Attorneys, Judges, Clerk of Courts, Jailers, Probation and Parole and more.
Tentative agenda is:

Casey Anthony Case   *Sovereign Citizens-West Memphis Shooting*
TIME/Interface Updates   *Media Relations*
WI Crime Labs   *Creating a Respectful Work Environment*
Audits   *Active Shooters in Schools & Public Settings*
Stress/Trauma Exposure for Dispatchers   *And more...*

New this year
Tuesday September 10th
Early Registration & Vendor Reception 4-7pm
Screening of movie "Heroes Behind the Badge" 7pm

2013 Presenters:

Bob Plaudert
Former Chief of Police & Father to Sgt. Brandon Plaudert killed in the line of duty by Sovereign Citizens

Major Ron Stucker
A 25 year veteran of the Orange County Sheriff's Office in Orange County, Florida and a Veteran of the United States Air Force

COMMENTS FROM PREVIOUS ATTENDEES:
"Another good conference!"   "Very well put together"
"Very good information"   "CIB conference keeps getting better"

Online registration, registration forms, hotel and detailed conference & vendor information is available at http://www.doj.state.wi.us/dles/cib/conference/annual-cib-conference

Real ID

The Wisconsin Department of Transportation recently began issuing driver's licenses and ID cards in compliance with federal Real ID requirements. Congress passed the REAL ID Act in an effort to strengthen the security, authentication and issuance standards for state driver's licenses and ID cards.

Beginning at some point within the next five years, it is expected that federal agencies will accept only a driver's license or ID card issued in compliance with the REAL ID Act as identification for official federal purposes such as boarding federally regulated commercial aircraft, accessing federal facilities that require identification to enter or entering nuclear power plants.

Wisconsin Real ID compliant driver's licenses and ID cards are marked with a gold star in the upper right corner. Wisconsin will continue to issue driver's licenses and ID cards that are not Real ID compliant. Aside from the star, both Real ID compliant and not compliant cards look the same.

For more information visit www.wisconsindmv.gov. Questions should be directed to Kristina Boardman, DMV Bureau of Field Services Director, at 608-266-5082 or email at kristina.boardman@dot.wi.gov.

WCAN: WI Crime Alert Network

By now your agency should have heard of the Wisconsin Crime Alert Network, a service of the Wisconsin Department of Justice. The Wisconsin Crime Alert Network (WCAN) allows local, state, federal and tribal law enforcement agencies to send out crime alert bulletins to businesses and the public, targeting recipients based upon type of business and location. The Wisconsin Crime Alert Network aids law enforcement officers in the apprehension of criminals by providing a rapid, cost-effective means of communication between law enforcement agencies and the communities they serve.

Businesses and members of the public that wish to receive alerts can subscribe for a $12 annual fee. There is no cost to Wisconsin law enforcement agencies/officers that wish to use the network to send or receive messages.

The Wisconsin Crime Alert Network is a valuable tool for law enforcement and has already had numerous success stories to its credit. Agencies are reminded, however, that the network is *not* a replacement for the TIME System. Alerts sent on the Wisconsin Crime Alert Network are sent only to those law enforcement agencies/personnel that have subscribed and are in the geographic area selected by the sender, thus not every law enforcement agency will receive crime alerts.

In addition, because alerts sent on the Wisconsin Crime Network are received by the general public, sending agencies must be careful to abide by TIME/NCIC policies and state/federal laws regarding information dissemination. For example, state statutes closely restrict the use and dissemination of Wisconsin driver's license photos, effectively prohibiting their use in a crime alert.

For further information about the Wisconsin Crime Alert Network, or to subscribe, visit www.wisconsincrimealert.gov.

Portal 100 Access

CIB receives numerous calls from agency administrators reporting a problem: their new employee has completed the required TIME System training, but when the employee attempts to log on to the Portal 100 software, they are unable to do so. The user instead receives an error message indicating they are not authorized. In most cases, investigation reveals the reason for the problem: no one requested Portal 100 access for the user.

An agency administrator *must specifically request* Portal 100 access for a user. New users are not automatically granted Portal 100 access when added to an agency's roster. When requesting Portal 100 access for a user, it is also important to indicate what *level* of access is desired. Three levels of Portal 100 access are available:

1) Standard user level access.
4) Printer level access. The level 4 user can change print options, and message handling options.
9) Administrator level access. The level 9 user is able to perform system level setup functions, adding ORIs, message logging, changing printers, etc.

NCIC Images

They say a picture is worth a thousand words and with the ability to associate images with NCIC entries, your agency can speak volumes. An image should be entered for a person or property when it will assist in identification of either. The types of images that can be associated with a person record are mugshot, signature, and identifying images. Stolen property entries, such as articles, parts, boats and vehicles can be associated with an identifying image. Generic images are also available for use with vehicle or boat entries.

Mugshot: a frontal face view from the shoulders to the top of the head maintained by an ORI and associated to a person.

Signature: an image of a signature.

Identifying image: an image which may help identify a person or property (e.g., scars, marks, and tattoos; photograph of a person; "aged" photograph of a missing juvenile; photograph of a vehicle or an article; etc.)

Generic image: an image entered and maintained by the FBI as a general reference for a vehicle or boat.

When the image is entered, the NCIC number (NIC) of the person or property record must be included. The NIC is the link between the image record and the person or property record. Wisconsin driver's license photos may *not* be entered as an NCIC image. Images must be in .jpg format. Images are subject to the same validation requirements and retention periods as the records they are associated with.

When a user queries a person or property, they may request that image information be returned *if available* by indicating 'Y' for yes in the NCIC image indicator field. For a person, this would be a mugshot; for property, it would be either the identifying image or the generic image. If a user wants to view all images associated with a record (identifying images for a person, etc.) they must use the query image transaction #0017 and query the NIC of the record in question.

Violent Person File

NCIC has introduced a new file. The Violent Person File was created for the purpose of enhancing officer safety by providing a warning to law enforcement about individuals who have a propensity for violence against law enforcement officers. The file is queried as part of a standard wanted person query. A notification is sent to the holder of the record when a positive hit is generated. Law enforcement will be able to make entries to this file for those who meet at least one of the criteria:

1. Offender has been convicted for assault or murder/homicide of a law enforcement officer, fleeing, resisting arrest, or any such statute which involves violence against law enforcement.
2. Offender has been convicted of a violent offense against a person to include homicide and attempted homicide.
3. Offender has been convicted of a violent offense against a person where a firearm/weapon was used.
4. A law enforcement agency, based on its official investigatory duties, reasonably believes that the individual has seriously expressed his or her intent to commit an act of unlawful violence against a member of the law enforcement or criminal justice community.

CIB is in the process of updating the Portal 100 software to include entry/cancellation of Violent Person File records and expects the forms to be available in late spring 2013. A sample of a response from the Violent Person File is shown here. Please note that the warning caveat will differ depending on what criteria were indicated on the record entry.

```
WARNING-A SUBJECT IN THIS RESPONSE HAS BEEN IDENTIFIED AS A VIOLENT OF-
FENDER OR A SERIOUS THREAT TO LAW ENFORCEMENT OFFICERS. REVIEW THIS RE-
SPONSE IN ITS ENTIRETY TO OBTAIN ADDITIONAL INFORMATION ON THIS SUBJECT.
USE EXTREME CAUTION IN APPROACHING THIS INDIVIDUAL.

***MESSAGE KEY QW SEARCHES WANTED PERSON FILE FELONY RECORDS REGARDLESS OF
EXTRADITION AND MISDEMEANOR RECORDS INDICATING POSSIBLE INTERSTATE EXTRADI-
TION FROM THE INQUIRING AGENCY'S LOCATION. ALL OTHER NCIC PERSONS FILES ARE
SEARCHED WITHOUT LIMITATIONS.
WARNING-THE SUBJECT IN THIS RECORD HAS BEEN IDENTIFIED AS A VIOLENT OF-
FENDER. THE SUBJECT HAS A CRIMINAL HISTORY OF ASSAULTING LAW ENFORCEMENT
OFFICERS. USE CAUTION IN APPROACHING THIS INDIVIDUAL. DO NOT ARREST OR DE-
TAIN BASED SOLELY UPON THIS INFORMATION.

MKE/VIOLENT PERSON
CMC/05 - VIOLENT TENDENCIES
ORI/VASP01000 NAM/SMITH, JOHN J SEX/M RAC/W DOB/19511012
HGT/510 WGT/175 EYE/BRO HAI/BRO FBI/123456789 SKN/DRK
SMT/SC R HND
FPC/121011CO141159TTCI13 MNU/AS-123456789 SOC/123456789
OLN/11111111 OLS/MD OLY/1999
VPC/1-ASSAULT ON LAW ENFORCEMENT
OCA/123456273
MIS/KNOWN TO THREATEN POLICE OFFICERS
ORI IS VA STATE POLICE ROANOKE OFFICE 703-555-1212
NIC/L146203706    DTE/20121204    DLU/20121204
```

Oh Canada

Drive north far enough, and you'll hit…Canada. Users are reminded they have access to Canadian information via the TIME System.

The TIME System provides users with access to information on Canadian persons, criminal history, vehicles, boats, parts, guns, articles and securities.

The Canadian setup is similar to the United States setup in that there is a nationwide system (CPIC – Canadian Police Information Centre, similar to NCIC) and separate databases for each province (state). For example, when querying a vehicle here in the US users will receive responses from both NCIC (stolen status, etc) and the state (vehicle registration, etc.), users querying a Canadian vehicle will receive responses from both CPIC (stolen status, etc.) and the province (vehicle registration). The format of the response may differ, just as the formats of responses from various US states differ.

Is Your AAI Really an AAI?

Anyone who accesses the TIME System, no matter how that access is obtained (*e*TIME, MDC, Portal 100 software, interface agency software, etc.), must be trained and tested. With over 23,000 active TIME System users accessing the TIME System at any point in time, there is no way each user could attend a certification class led by a CIB instructor.

CIB created the concept of an Agency Assigned Instructor (AAI) to help fill the gap. Agencies may designate a person or persons to serve as an AAI. The AAI conducts MDC level TIME System certification and recertification classes, presenting instructional material and administering the exams. Results of the exams are forwarded to CIB for credit.

In order to serve as an AAI, a person must have a current TIME System certification *at the Basic or Advanced level*. They *must also* have attended a specialized AAI class led by a CIB instructor, where they will receive the needed instructional materials, etc. CIB has discovered subjects from several different agencies that have been providing MDC instruction and certification *even though they have not met the requirements* to be an AAI.

Please ensure your AAI is fully qualified to present the needed certification instruction. If they are not a qualified AAI, the MDC certification of users who have attended their classes may be considered invalid.

The Public & TIME/NCIC Information

Recent questions from TIME System users indicate a need to revisit TIME System policy with regard to public access to TIME/NCIC information. In certain circumstances, agencies may release TIME System status information to the public. Agencies should ensure their personnel are familiar with the rules below regarding release of TIME System information to the public.

-It is up to the local agency's discretion as to whether to participate and handle requests from the public.

-Agencies are prohibited from releasing actual TIME/NCIC System responses. Agencies may only release information about the type of record (wanted, missing, stolen, etc.), status of the record, and name of the originating agency of the record. If the requestor wants additional information about the record they should be referred to the record originating agency.

-Certain types of TIME/NCIC information are confidential and *may not be acknowledged or released*. This includes: Juvenile information
>   Wisconsin Department of Transportation information
>   Wisconsin criminal history record information
>   NCIC III criminal history information
>   NCIC Supervised Release File information
>   NCIC National Sex Offender Registry information
>   NCIC Gang File information
>   NCIC Known or Appropriately Suspected Terrorist File information
>   NCIC Immigration Violator File information
>   NCIC Protection Order File information that is inactive/historical
>   NCIC Identity Theft File information
>   NCIC Protective Interest File information
>   NCIC Person With Information data (associated with missing person records)

-Advertising/commercial dissemination of TIME/NCIC data is prohibited, however agencies may charge a nominal fee for processing these requests.

CIB also recommends that when returning the results to a public requestor, the agency include a disclaimer, such as "These results are based solely on the information provided and this agency cannot guarantee that the person or property represented in the response is or is not the person or property you are interested in. Additional information may be available within local agency records."

Where, Oh Where?

Do you know where your TIME System router is? Chances are, your agency's TIME System router is a piece of equipment that you very rarely think of – until there is a problem. When there is a problem with your agency's TIME System access, one of the first things a technician will need to locate is the TIME System Badgernet router. Unfortunately, all too often agency personnel do not know where it is located. Please ensure that all personnel know the location of this important piece of equipment.

Entries Expire

With the turn of the new year, it is a good time to remind TIME System users that not every TIME/NCIC System entry remains on file forever. Retention periods are set for various types of entries. Remember to include as much information as possible in your entry, as many times the information included determines how long an entry remains on the system.

|	
Wanted Person:	Warrant - indefinite
	Temporary felony want - 48 hours
	Temporary misdemeanor want - 72 hours
	Detainers - midnight of date sentence ends
Missing Person:	Indefinite
POIF:	Temporary orders - 96 hours after expiration date of order
	Injunctions - midnight of expiration date
Gang Organization:	Indefinite
Gang Member:	Date of purge entered or 5 years
Unidentified Person:	Indefinite
Identity Theft:	Date of purge entered or 5 years
Vehicle:	Stolen, if VIN or OAN included - 4 years + year of entry
	Stolen, if VIN or OAN is not included - 90 days
	Felony - 90 days
	Stolen/missing license plate - 4 years + year of entry
Part:	4 years + year of entry
Article:	1year + year of entry
	Indefinite for entries with type code of T, Q & Z
Gun:	Stolen/lost/felony - indefinite
	Recovered - 2 years + year of entry
Boat:	If BHN included – 4 years + year of entry
	If BHN is not included - 90 days
Security:	4 years + year of entry
	Travelers checks/money orders - 2 years + year of entry

Transsexual Wanted Person Entries

Several agencies have contacted CIB for guidance on how to enter a warrant for a subject who is transsexual – for example a warrant exists for the subject as a male, however the subject is now anatomically female.

The name and identity on the warrant guides the entry. Thus, if the warrant was issued for a male, it must be entered into the system that way. The female name could then be entered as an alias. The fact the subject is transsexual should then be listed as a scar/mark/tattoo, and NCIC suggests the agency use the miscellaneous remarks field to indicate the sex of the individual at birth and what sex they are at the time the record is entered.

Agencies in this situation may wish to consult with the court that issued the warrant to determine if a new warrant should be issued for the subject listing their current identity.
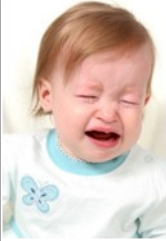
CHRI and Purpose Code E

The TIME System can be used for non-law enforcement background checks, *provided there is a law* (federal, state or local ordinance) requiring the background check. The correct purpose code to use when conducting such background checks is purpose code E.

III, the Interstate Identification Index, does not allow the use of purpose code E to access III information, and users may not use another purpose code to 'get around' this prohibition.

Purpose code E is allowed when querying Wisconsin criminal history record files. Only Wisconsin adult criminal history record information is returned when purpose code E is used. Other states also allow the use of purpose code E, and transactions are available in the Portal 100 software for use in checking another state's central repository for criminal history record information.

Partial Photos

In the past, if a driver's license photo was too large to be transmitted via the TIME System or *e*TIME browser, the user would receive an error message. A change was recently made that allows an oversized photo to be displayed. If the Wisconsin driver's license photo is larger than system limits, the system will display as much of the photo as possible. This will result in users seeing a partial/cropped photograph.

Deadlines, Advanced Authentication & IPSec

The FBI has extended the interim compliance requirement for advanced authentication from a police vehicle until September 30, 2014, section 5.6.2.2.1 of the CJIS Security Policy. This extension does not apply to new implementations or upgrades as defined by the CJIS Security Policy section 5.6.2.2.2 (6). An upgrade includes implementation of new technology, implementation of encryption, or an upgrade exceeding 25% of the cost of the original system.

If your agency does not have advanced authentication in place for this portion of your network, you should be working toward implementing an approved method of advanced authentication, such as biometric systems, user-based public key infrastructure (PKI), smart cards, software tokens, hardware tokens, or risk based authentication. Many agencies had implemented a Virtual Private Network (VPN) with Internet Protocol Security (IPSec) to meet the advanced authentication requirements of previous versions of the CJIS Security Policy. These agencies must also meet the new advanced authentication requirements by September 30, 2014.

Questions about advanced authentication and its implementation can be directed to Chris Kalina, TIME System Operations Coordinator at 608-266-7394 or via email to kalinaca@doj.state.wi.us.

CIB Contact List

	Name	Telephone	Fax Number	Email
Director	Walt Neverman	608-264-6207	608-267-1338	nevermanwm@doj.state.wi.us
Deputy Director	Dennis Fortunato	608-267-2235	608-267-6200	fortunatodj@doj.state.wi.us
TIME & Tech. Serv. Mgr.	Courtney Doberstein	608-266-0872	608-267-1338	dobersteincl@doj.state.wi.us
Training Officer	Donna Bente	608-264-9452	608-267-1338	bentedl@doj.state.wi.us
Training Officer	Jim Muller	608-261-5800	608-267-1338	mullerjj@doj.state.wi.us
Training Officer	Jessica Sash	608-266-9341	608-267-1338	sashjl@doj.state.wi.us
TIME Operations Coord.	Chris Kalina	608-266-7394	608-267-1338	kalinaca@doj.state.wi.us
TIME & *e*TIME Analyst	Mary Moroney	608-266-2426	608-267-1338	moroneym@doj.state.wi.us
TIME & *e*TIME Analyst Validation	Sara Phelan	608-266-7955	608-267-1338	phelansm@doj.state.wi.us
Livescan Analyst	Joan Wolfe	608-264-9490	608-267-1338	wolfejk@doj.state.wi.us
Supplies and Imaging	Carol Brown	608-266-9585	608-267-4558	brownca@doj.state.wi.us
TIME Billing	Chris Kalina	608-266-7394	608-267-1338	kalinaca@doj.state.wi.us
Fingerprint ID-AFIS (WI Crime Lab – Milwaukee)	Adrianna Bast	414-382-7500	414-382-7507	bastar@doj.state.wi.us
Record Check	Vacant	608-267-2776	608-264-6200	
Criminal Records	Mary Meyer	608-266-9561	608-261-0660	meyerma@doj.state.wi.us
Firearms Unit	Capri Lione	608-267-2776	608-264-6200	lioneca@doj.state.wi.us
TRAIN	Kristi Hammes	608-266-7792	608-267-1338	cibtrain@doj.state.wi.us

Check the CIB website for additional data at: www.wilenet.org