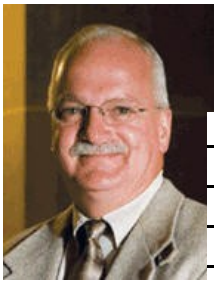
Wisconsin Department of Justice
Division of Law Enforcement Services

J. B. Van Hollen
Attorney General

VOLUME 2012-3
NOVEMBER 2012

TIME System Newsletter
Crime Information Bureau



The 2012 CIB Conference was held Sept 19th – 21st at the Radisson Hotel & Conference Center in Green Bay. Based on comments I received and the evaluations turned in, the conference was another success and I look forward to seeing all of you again next year.

The CJIS Security Policy establishes a minimum set of controls to protect criminal justice data. The Wisconsin Department of Justice is the CJIS Systems Agency for Wisconsin and is responsible for ensuring compliance with the CJIS Security Policy by all Wisconsin agencies having access to CJIS data. The FBI CJIS Division released a revised CJIS Security Policy on July 13, 2012, version 5.1. Version 5.1 primarily changed some terminology from version 5.0, in addition to clarification of policy regarding background check requirements for persons that are not Wisconsin residents. This clarification allows for a name based criminal history check to the other state of residence in addition to the Wisconsin and national fingerprint based background check. See section 5.12.1.1 of the CJIS Security Policy version 5.1 for the specific language.

The CJIS Security Policy contains a couple of policies that are effective in January 2013 you should be aware of. The first is a topic that has been discussed for a number of years, advanced authentication. In January 2013 the provision that allowed agencies to use a VPN with IPSec for advanced authentication that was implemented pursuant to version 4.5 of the CJIS Security Policy will expire. Agencies that operate an interface to the TIME System using wireless, radio transmission, Internet, or dial-up must implement an alternative method of advanced authentication as defined by the CJIS Security Policy. Advanced authentication adds additional security to the standard userid and password due to the higher risk of these transport methodologies. The Department of Justice has already deployed an acceptable method of advanced authentication in the eTIME Browser application. Check with your appropriate personnel to ensure your compliance. The second topic is the requirement for non-terminal agency users to complete security awareness training if they have access to FBI CJIS data through an agreement with a TIME System terminal agency. Example: If your agency has no direct TIME System access but utilizes a central dispatch center to run TIME System queries your personnel will need to complete Security Awareness training starting in January 2013. If you need a copy of the latest CJIS Security Policy please contact Chris Kalina at kalinaca@doj.state.wi.us. 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

Walt Neverman
Director CIB

INSIDE THIS ISSUE:

2013 CJIS Security Requirements

The new year is rapidly approaching, and with it comes new requirements under the CJIS Security Policy. Below is a list of the new requirements. Each is followed by the specific CJIS Security Policy section reference. Agencies should ensure they and their information technology staff are aware of these changes and are actively working to meet these requirements:

- Use of existing VPN's with IPSec to meet advanced authentication requirements from a police vehicle no longer allowed (5.6)
- Police vehicles no longer considered a physically secured location (5.8)
- Users must acknowledge a system use notification before login (5.5)
- Specific information must be logged regarding specific computer events, these audit records must be time stamped when generated (5.4)
- System must be in place to alert agency if logging fails (5.4)
- Event logs must be reviewed at least once a week, and these audit records must be retained until no longer needed (5.4)
- Network access control policies must be in place (5.5)
- Access to privileged functions must be restricted to explicitly authorized personnel (5.5)
- Encryption of stored data required if agency cannot meet physical and personnel security requirements (5.8)
- Monitoring/boundary protection required (5.10)
- Information must be encrypted if at rest outside the boundary of the physically secure location (5.10)
- Intrusion detection tools and techniques must be employed (5.10)

New Temporary Plate Design

A new temporary license plate design is now available for customers who complete an online application to title and register an automobile or light truck using a new web system: EMV Public.

One plate is printed by the customer on 8½x11 inch standard paper. The words "WISCONSIN TEMPORARY PLATE" are at the top, followed by the plate number in white on a black background. The vehicle make, model, year and last six digits of the VIN are printed next to the plate expiration date. The plate is valid for 90 days from the day the application is completed online or until the customer receives regular metal license plates from the Department of Motor Vehicles.

Customers are instructed to display the plate in the inside lower driver's side rear window. This is permitted by administrative rule 132.04.

The new temporary plate, owner and vehicle information are available immediately in a TIME inquiry. The license plate type code for inquiry is IT.

At this time this EMV Public service is only available for individuals who purchase a vehicle through a private sale that is currently titled in Wisconsin.

Loooong Names

We've all probably heard the song "John Jacob Jingleheimerschmitt. Longer names are becoming a part of life as our world expands to include names from other cultures and hyphenated names. In fact, the Wisconsin Department of Transportation has begun to issue driver's licenses/identification cards with truncated names printed on the card itself as the full name is too long to display. TIME System users need to be aware of how these long names are dealt with in the various files routinely searched on a person query.

The CIB files treat each part of a name as a separate field, each field allowing up to 30 characters:

Last name: Averyveryveryreallylonglastname
First name: John
Middle name: Jacob

However, NCIC files combine the name into one long string, the total length of which cannot exceed 30 characters:

Name: Averyveryveryreallylonglastn, J

Notice how the last and first names are cut off due to the length and format requirements of NCIC.

What does this mean for TIME System users? If you enter a wanted person record for a subject with a very long name, be aware that while the CIB response may show the entire name, the name shown on the NCIC record may be truncated to meet NCIC requirements.

Vendors/Contractors

Does your agency use a vendor or contractor for information technology services, paper shredding, or hardware disposal? If so, be certain you are meeting the security requirements:

- Have the required fingerprint based background checks been conducted on the vendor/contractor employees? If the vendor/contractor employee resides in a different state than that of the criminal justice agency, they must also conduct an NLETS CHRI query to the appropriate state.
- Has each vendor/contractor employee completed the required security awareness training?
- Has each vendor/contractor employee signed the required security addendum (found at the end of the Management Control Agreement)?

If you answered 'NO' to any one of these conditions, your agency may be out of compliance with CJIS Security Policy, and should take steps to complete the missing items. A sample Management Control Agreement and the Security Awareness Handout can be found on the CIB website at: https://wilenet.org/html/cib/manuals-forms/index.htm.

What Disqualifies a Person?

CIB's Firearms Unit is responsible for conducting background checks on handgun purchasers and CCW license applicants in Wisconsin. To do so, the Firearms Unit staff consult several sources of information, including the TIME System, criminal history records, etc. Some information or criminal history record information may require clarification, resulting in a Firearms Unit staff member contacting your agency to obtain further information about an incident. So what disqualifies someone from purchasing a weapon/obtaining a CCW license? Here is a list of state/federal disqualifiers:

- Convicted of a felony in this state, or convicted of a crime elsewhere that would be a felony if committed in this state, or adjudicated delinquent for an act that if committed by an adult in this state would be a felony.

- Found not guilty of a felony in this state by reason of mental disease or defect, or found not guilty for a crime elsewhere that would be a felony in this state by reason of insanity or mental disease, defect or illness.

- Convicted in any court of a crime punishable by imprisonment for a term exceeding one year.

- Misdemeanor convictions if the maximum sentence exceeds 2 years prison.

- Convicted in any court of a misdemeanor crime of domestic violence that includes the use or attempted use of physical force, or the threatened use of a deadly weapon and was committed by a current or former spouse, parent, or guardian of the victim, a person with whom the victim shared a child in common, a person who was cohabiting with or had previously cohabited with the victim as a spouse, parent, or guardian or a person who was similarly situated.

- Enjoined under an injunction issued under s. 813.12 (domestic abuse) or s. 813.122 (child abuse) , ordered not to possess a firearm under s. 813.125(4m) (harassment injunction) or subject to a court order injunction restraining the subject from harassing, stalking, or threatening an intimate partner or child of such partner.

- Fugitive from justice (any felony or misdemeanor warrant). Non-criminal warrants (e.g. traffic) are not disqualifying.

- An unlawful user of or addicted to any controlled substance. This can be shown by any possession of a controlled substance conviction within the past year (including misdemeanor and non-criminal convictions), a drug paraphernalia conviction in the past year, provided the paraphernalia tested positive for the controlled substance (including misdemeanor and non-criminal convictions), an open case involving drugs, provided the drugs or the defendant tested positive for the controlled substance within the past year, any admission of drug use or possession by the defendant in the past year (contained in a police incident report or criminal complaint) or an Operating While Intoxicated (OWI) conviction in the past year, provided the intoxicant was a controlled substance.

- Adjudicated as mental defective, committed to a mental institution, or committed for treatment under s.51.20(13)(a) and ordered not to possess a firearm under s.51.20(13)(cv)1., or ordered not to possess a firearm under s.51.20(13)(cv)1., 51.45(13)(i)1., 54.10(3)(f)1., or 55.12(10)(a).

- Under indictment or information for a crime punishable by imprisonment for a term exceeding one year, or a military service member charged with any offense punishable by imprisonment for a term exceeding 1 year if referred to a general court martial. (Disqualifies for gun purchase only).

- Discharged from the Armed Forces under dishonorable conditions.

- Alien illegally in the US.

- Renounced US citizenship.

New Process for WI DL/ID Cards

Law enforcement agencies should be aware of changes in the process of issuing/ renewing Wisconsin driver's licenses and identification cards. In 2012 the Wisconsin Department of Transportation began a process called "central issuance" for all driver licenses and ID cards.

What does this mean? DOT customers will not be issued a permanent license or identification card when at the DOT service center. Instead, all driver's license and identification card products will be mailed from one production facility to the card holder's home address. Customers should receive their driver license or ID within 10 business days.

Customers will leave the DMV service center with a paper receipt that is valid for 45 days. The receipt, including a photo, is acceptable photo identification for voting and serves as the license or ID until the permanent card arrives in the mail. Customers who are renewing an existing license or ID card will also leave the DMV service center with their expired (or soon to be expired) card, invalidated with a hole punch by the DMV processor. A sample of the receipt is seen here.

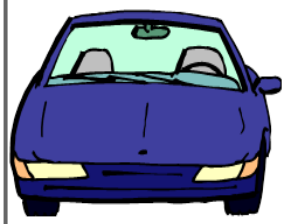
In addition, Wisconsin driver licenses and ID cards have been redesigned. The background security design will look different, and will include an image of the Wisconsin State Capitol. In addition to the primary portrait, there will be two "ghost images," one color and one laser-engraved. The back of the products will again include a 2D bar code with printed data from the front of the card, and the writable surface for an anatomical gift statement is still available. A sample of the new style license is shown here.

Policy Requirements

When was the last time your agency updated its policy manual? For many agencies such updates happen only once a year, or once every several years.

Agencies that access the TIME/NCIC Systems are required to have written policy covering numerous topics, such as validation, discipline, information technology, etc. If your agency policies have not been updated recently, you may be missing some of these required policy provisions.

Rather than re-invent the wheel, agencies are reminded that CIB has prepared a sample TIME System policy document that covers all the required topics and more. This sample policy is posted on the CIB website at https://wilenet.org/html/cib/manuals-forms/index.htm. You may need to scroll to the bottom of the page to locate the policy. The document is available in both pdf and Word format.



National Motor Vehicle Titling Information System

Law enforcement investigations have shown that criminals involved in domestic auto theft enterprises often perpetrate violent crimes, such as homicide, drug trafficking, human trafficking, and terrorism. The National Motor Vehicle Title Information System (NMVTIS) is, among other things, a tool that assists local, state, and federal law enforcement in investigating, deterring, and preventing vehicle-related crimes. NMVTIS was established by the Anti-Car Theft Act of 1992 (Public Law 102-519), the Anti-Car Theft Improvements Act of 1996 (Public Law 104-152), and its implementing regulations (28 CFR part 25, published January 30, 2009, 74 FR 5740). It is an electronic system designed to protect consumers from fraud and unsafe vehicles and to keep stolen vehicles from being resold. NMVTIS captures specific pieces of vehicle information from state motor vehicle titling agencies, automobile recyclers, junk and salvage yards, and insurance carriers into one system.

Vehicle theft and cloning have become a lucrative business for organized criminals with the profits often used to fund additional criminal activity and terrorism. The NMVTIS Law Enforcement Access Tool provides law enforcement with the information necessary to investigate vehicle-related crimes. The NMVTIS Law Enforcement Access Tool assists law enforcement with:

- Investigating vehicles involved in violent crimes, smuggling (narcotics, weapons, and currency), and fraud
- Identifying vehicle theft rings
- Increasing the identification of other criminal enterprises involving vehicles

Law enforcement agencies have two options to access the NMVTIS Law Enforcement Tool: the Regional Information Sharing Systems (RISS) or Law Enforcement Online (LEO). Law enforcement access to NMVTIS data is available at no cost to law enforcement. If you are a law enforcement agent or investigator and would like to obtain instructions for accessing NMVTIS data, please email NMVTIS@usdoj.gov.

Do You Pass It On?

Many law enforcement agencies in Wisconsin provide TIME System service or information to other authorized criminal justice/law enforcement agencies that do not have TIME System terminals of their own. The most common scenario is a sheriff's department that provides dispatching services to a local police department and provides them with TIME System printouts such as driver's record information, criminal history record information, etc.

Agencies should be aware of a new requirement for training under the FBI CJIS Security Policy. Beginning in 2013, anyone who has access to CJIS data, *even those at non-terminal agencies*, must complete security awareness training. Agencies in this situation may need to ensure personnel at non-terminal agencies have completed needed security awareness training to ensure TIME System information provided to non-terminal agencies is kept secure.

Security awareness training can be completed either online on CIB's TRAIN website, or is also available on paper. As with other TIME certifications, security awareness training must be renewed every 2 years. The Security Awareness Training Handout is available on CIB's website, https://wilenet.org/html/cib/training-calendar.htm.. If your agency chooses to use the paper version of security awareness training, a copy of each person's signed Security Awareness Certification Statement must be kept on file at the department as proof the training has been completed.

State Traffic Operations Center

Wisconsin Department of Transportation State Traffic Operations Center (STOC) handles traffic management for the state of Wisconsin. The physical Operations Center is located in Southeastern Wisconsin in the City of Milwaukee. The STOC is staffed 24 hours per day, 7 days per week and communicates regularly with sheriff, fire, police, and Wisconsin State Patrol, as well as media outlets and construction project managers.

From the STOC, it is possible to use various traffic management tools, such as: closed circuit television units, traffic condition cameras, ramp meters, variable message signs, highway advisory radio, roadway sensors and other tools. The STOC is designed to improve the safety and efficiency of the freeway system by reducing incidents and relieving traffic congestion.

Traffic condition cameras provide live video of traffic conditions. This video pinpoints congestion areas and enables emergency dispatchers to provide personnel with location and incident information. Traffic condition cameras on top of 45-foot poles are strategically placed along the freeway system. Cameras can be found at the following locations: Fond Du Lac, Milwaukee area, Madison area, Green Bay area, and Rock County. The STOC can be reached via TIME System administrative message to mnemonic 'STOC' or at the following address:

State Traffic Operations Center
433 W. St. Paul Avenue, Suite 300
Milwaukee, Wisconsin 53203
(414) 227-2166
statewide.toc@dot.wi.gov

New Field on Stolen Vehicle Records

TIME System users may have noticed a new field that is appearing on NCIC stolen vehicle responses: OPT/

This field indicates whether or not the information in the stolen vehicle record can be included on a website that is being created for the public. This website would allow the public to check the status of a vehicle prior to purchase, etc. The website is still in development and not yet functional, but NCIC has made this change in preparation for future release of the site.

All Wisconsin stolen vehicle entries will be defaulted behind the scenes to indicate OPT/IN (information can be included on the public site). This policy determination was made by the TIME Advisory Committee at their 2012 meeting.

Only 3 Reasons

TIME System agencies are reminded that per state statute 175.60(12) agencies are only allowed to access concealed carry license information available via the TIME System for three reasons:

1. To confirm that a license or certification card produced by an individual at the request of a law enforcement officer is valid.
2. If an individual is carrying a concealed weapon and claims to hold a valid license or certification card but does not have the license or certification card, to confirm that the individual holds a valid license or certification card.
3. To investigate whether an individual submitted an intentionally false statement during the license application process.

Temporary Felony Want

The TIME/NCIC Systems allow for entry of a wanted person record even if no warrant has been issued in special circumstances. Agencies that have knowledge by police that a felony was committed and who the person was that committed the felony but no warrant has been issued yet may enter the subject as a wanted person in the Temporary Felony category while the process for obtaining a felony warrant is pursued.

The want can be entered into CIB only or CIB and NCIC, and the entry remains on file for 48 hours before being automatically purged. As the entry remains on the system for such a short amount of time, agencies are not allowed to add detainer information to such a record.

Its One or the Other:

Authorized personnel or visitor. Under CJIS Security Policy, when it comes down to subjects having access to your agency's physically secure area, people fall into one of these two categories: they are either authorized personnel or visitors.

Authorized personnel have had the required fingerprint based background check *and* have completed the required security awareness training *and* are on your agency's list of those with authorized access.

Visitors are those persons who do not meet the requirements for authorized personnel.

Authorized personnel can have unescorted access to your agency's physically secure area.

Visitors must be escorted at all times when accessing your agency's physically secure area and their visit must be logged. The visitor log must contain the person's name and agency, form of identification, date of access, time of entry and departure, purpose of visit, name and agency of person visited. The visitor access records must be frequently reviewed for accuracy/completeness.

Many agencies have questioned some common scenarios: What about school tours of the department? How about confidential informants entering the physically secure area? Cleaning crews? Officers from other departments? All of these personnel would be considered visitors subject to the escorting and logging requirements. Yes, even officers from other departments are considered visitors unless you can verify they have completed the background check, completed security awareness training, and been added to your agency's list of authorized users. This verification could come in the form of a letter/list from their department specifying what officers have met the requirements. The letter has to be specific, listing individual names, it cannot just say 'all officers from the department have completed requirements'.

Once you have verified they have met the requirements you can add them to your list of authorized users, and remember your list of authorized users has to be kept up to date. Same rules apply for building services and IT - either they have completed the background check and security awareness training and thus can have unescorted access to your physically secure area, or if they have not done those things they are considered visitors and must be escorted and logged.

N-DEx Audits

N-DEx (National Data Exchange) is a criminal justice information sharing system implemented by the FBI's CJIS (Criminal Justice Information Services). Similar to Wisconsin's WIJIS Gateway, N-DEx provides tools for law enforcement to search, link, analyze and share criminal justice information such as incident/case report data, arrest data, booking/incarceration data and probation/parole data on a national basis. Agencies nationwide contribute data to N-DEx, including federal agencies and entire state systems. N-DEx is operational 24 x 7 and continues to grow in number of records and functionality.

Query access to N-DEx today is limited and only accessible via the CJIS Law Enforcement Online (LEO) site. Your agency is not required to contribute records to N-DEx to be approved to query N-DEx. N-DEx agencies are now subject to required training and audits mandated by the FBI, and can expect to receive a packet of audit materials from CIB to be completed and returned.

Making a List, Checking It Twice

Agencies are reminded that the CJIS Security Policy requires that they validate their TIME System user accounts at least annually and document the validation. What does this mean for you? At least once a year, your agency must review and validate a list of all their TIME System users (which includes eTIME users, MDC users, Portal 100 users, etc.). This review should include removing access for those no longer actively using the TIME System, ensuring the appropriate access levels are assigned to each user based on their duties, ensuring the required background checks were completed, etc. Be sure and document in agency records that this validation has taken place, as confirmation of user validation may be required during a TIME System audit. Requests for removal of personnel from agency's TIME System roster can be sent to cibtrain@doj.state.wi.us

Enhanced Access to Oneida Vehicle Registration

Not all tribal vehicle registration information is readily available via the TIME System. Tribal license plates are issued by Indian nations in Wisconsin, *not* by the Wisconsin Department of Transportation. Vehicle registration information for these plates is stored in the database of the tribe, not the DOT database.

The Oneida Nation has now made their license plate/vehicle registration available to WI DOT, and thus to WI TIME System users. If users query an Oneida tribal license plate using a standard WI license plate query (0173) they will receive a record response containing information on the vehicle to which the license plate is assigned. License plate type code TB should be used for query purposes. The license plate type code used for entry of stolen/lost/missing Oneida tribal license plates is ZZ.

Updated information is uploaded to DOT on a daily basis. Any questions about Oneida tribal vehicle registration or the validity of Oneida tribal license plates should be referred to the tribe. A small number of Oneida tribal license plates (<300) may not return a record response. Additional information on Oneida Nation license plates can be found on the DOT website at www.wisconsindmv.gov.

Validation: Maybe You Need to Do It In Reverse…

Each month, agency validation officers are provided with a list of records that need to be validated during that time period. This list may include records for wanted person, missing person, stolen vehicles, etc. For many, the next step in the process is to provide a copy of the validation list to another person: for example, a copy of the wanted person list is given to the clerk of courts so they can verify the listed records are still backed up by a valid, active warrant.

But have you ever thought about doing validation in reverse? While not a TIME System requirement, reverse validation can help ensure all available records are entered into the TIME/NCIC databases. Reverse validation simply flips the source of the list: have the clerk of court send you a list of all cases with active warrants to check against your files. Have the detective division send you a list of all their open stolen vehicle cases for comparison. You may find that in some cases entries are not present on the system for some persons/property. In fact, a recent background check on a gun purchaser by CIB's Firearms Unit discovered just such a discrepancy: CCAP indicated a warrant existed for the subject, however a check of the TIME System found no associated wanted person record.

New Deputy Director

Attorney General J.B. Van Hollen appointed Dennis Fortunato to the position of Deputy Director of the Crime Information Bureau at the Department of Justice on April 30th, 2012. Dennis has been in the law enforcement field for over 32 years with the City of Fond du Lac Police Department. Dennis served the police department as a patrolman, then was promoted through various ranks, ultimately to the position of Assistant Chief of Police . Dennis has a Bachelors of Science Degree in Quality and Productivity Management and a Masters in Business Administration. He also attended the State of Wisconsin Executive Development Program and the 204th Session of the FBI National Academy executive program.

Now there is a Bridge

As your agency's needs change, there may come a time when someone who has an MDC level TIME System certification now needs to become Basic certified. In the past, this meant the person had to begin again – attending either a two-day Basic certification class, or completing online training modules 1-8.

CIB has re-evaluated this policy, and has determined there is an alternative. If an MDC certified TIME System user now needs to become Basic certified, they can do so by completing the online MDC recertification exam via TRAIN, and then also completing online training modules 7 & 8. This allows agencies greater flexibility in their personnel certification needs, while still ensuring that agency personnel are up-to-date on the needed subject matter.

DNR Citation Information

With deer hunting season almost upon us, more law enforcement agencies will be using the TIME System to access DNR information. Agencies are reminded that only citations issued between 1987 and January of 2010 are included with DNR person query responses. For complete record checks contact: PSN 1488 or WDNR via admin message, or email: lehotline@dnr.state.wi.us. The DNR and CIB are currently working jointly on a project to resolve this issue, with scheduled completion in December 2012.

CRIME INFORMATION BUREAU

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 – Madison)	Curt Bauer	608-261-8122 ext. 2600	608-294-2920	bauercj@doj.state.wi.us
Record Check	Mary Sturdevant	608-267-2776	608-264-6200	sturdevantmj@doj.state.wi.us
Criminal Records	Mary Meyer	608-266-9561	608-261-0660	meyerma@doj.state.wi.us
Firearms Unit	Mary Sturdevant	608-267-2776	608-264-6200	sturdevantmj@doj.state.wi.us
TRAIN	Kristi Prindle	608-266-7792	608-267-1338	cibtrain@doj.state.wi.us

Check the CIB website for additional data at: www.doj.state.wi.us/dles/cib