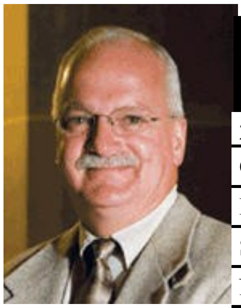
VOLUME 2012-1
MAY 2012

TIME System Newsletter Crime Information Bureau



As another year has passed, I look back and review what we have accomplished during that time. In 2011 we added the electronic sharing of Wisconsin driver photos via the TIME System. We also added the sharing of Wisconsin only warrants with other states that support those Nlets transactions, along with allowing you access to other states' in-state warrants. We completed our 2009-2011 audit cycle, which was a huge challenge considering the turnover of personnel and reduced staffing levels within the TIME & Technical Unit during that time. CIB also went live with issuing concealed carry licenses in November 2011 with query access via the TIME System for Wisconsin and out-of-state law enforcement personnel.

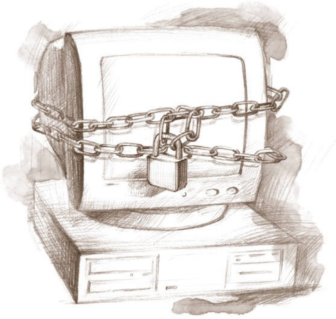
Phil Collins, a long time employee with CIB, transferred to the Department of Corrections in October 2011. Phil started in CIB as the TIME System Operations Coordinator, becoming the Operations Manager and eventually the Deputy Director for CIB. We wish him well in his new career. CIB's TIME & Technical Unit has some new faces. Courtney Doberstein has filled the TIME & Technical Services Manager position, my old position, and Kristi Prindle has filled the Operations Program Assistant position, Colleen's old position. Please see articles in this newsletter regarding our new staff.

2012 is already looking like a busy year with many proposed projects including new interfaces with the Department of Natural Resources and the Department of Corrections. The new interfaces will give us an opportunity to enhance the data sharing that already occurs with new technology but also consider adding new functionality such as probation/parole conditions, something law enforcement has been requesting for years. Wisconsin will be audited by the FBI in May and will include visits to some of your agencies. Additional requirements and changes to the CJIS Security Policy were effective in January 2012, please see additional articles on this topic in the newsletter.

The 2012 CIB Conference is Wednesday Sept 19th – 21st in Green Bay. Based on feedback I received at the conference and survey comments, last years conference was a success and I look forward to seeing all of you again this year.

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



2012 Is Here - and So Are New CJIS Security Policy Requirements

Though it seems like only yesterday, it has been over a year since CIB published the 'Special CJIS Security Edition' of the TIME System newsletter. As the last page of that special newsletter indicated, the coming of 2012 requires agencies to implement new CJIS security requirements. These requirements are summarized below. Details of these requirements can be found in the CJIS Security Policy Version 5.0, which is available on LEO or by request from CIB's Information Security Officer Chris Kalina (kalinaca@doj.state.wi.us).

- Agency agreements: agencies that provide system information to others are required to have a signed agreement in place. Specific language regarding information security is now required in these agreements. NOTE: the sample agency agreement available on the CIB website has been updated to include the required language.
- Visitor logging: agencies are now required to log visitors to their physically secure areas. The agency must maintain visitor access records to the physically secure location that include name and agency of the visitor, form of identification, date of access, time of entry and departure, name and agency of person visited and visit purpose.
- Information security incidents: agencies are now required to have an established operational incident handling capability for agency information systems that includes adequate preparation, detection, analysis, containment, recovery and user response activities. Other requirements, such as reporting, also exist.
- User accounts: agencies must validate user login accounts at least annually and document the validation.
- Identifier management: agencies must document the process for issuing user identifiers/ authenticators.
- Privileged functions: access to privileged functions must be restricted to explicitly authorized personnel (system administrators, etc.)
- Wireless protocols: numerous very specific requirements for wireless system access.
- Partitioning/virtualization: numerous very specific requirements for agencies using partitioning and/or virtualization as part of their network access.

New TIME & Technical Staff

Kristi Prindle joined the Crime Information Bureau on January 3, 2012 as an Operations Program Assistant. Kristi comes from a records management/customer service background. She began her career at UW Hospital working in medical records. Most recently she worked for the Department of Commerce, Environmental and Regulatory Services Division for over 11 years. Kristi managed bureau files, open records requests, and assisted in maintaining the database while working closely with the State Records Center and the DNR's Bureau of Remediation and Redevelopment. For seven years Kristi also owned and operated a successful eBay store where she sold jewelry of sterling silver and semi-precious stones of her own creation. While not working she enjoys open water fishing, reading, and spending time with her family, friends, and her dog Rowdy. Kristi is very excited to be with CIB and looks forward to serving the law enforcement community while continuing to serve the public.

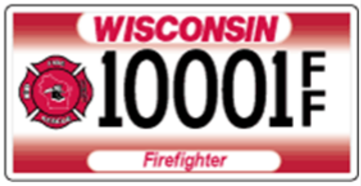
Concealed Carry Queries

On November 1st, 2011 Wisconsin Act 35 became effective and added issuance of concealed carry licenses to CIB's responsibilities. In addition to impacting CIB's daily duties, Act 35 impacts the TIME System as well. New TIME System transactions have been created to allow law enforcement personnel to access the concealed carry database under circumstances authorized by the statutes to check the current status of a license. Act 35 is very specific about when law enforcement is authorized to access this information and the requirements for control of the data.

Two new query transactions/screens have been created. For those using the Portal 100 software, the CCW query forms can be found on the menu in the Warrant/Wanted Persons file – Query Person Status Only. Transaction #0069 is used to query the status of a Wisconsin concealed carry license, and transaction #0070 is used to check the status of a concealed carry permit issued by another state. Here is a sample of a response from the Wisconsin file:

```
/0069 3479 626ACB01                  WI0130000
NHFS    98701     22 10/24/11 08:42 01 OF 01
***** CONCEALED CARRY WEAPON - LICENSE *****
STATUS=VALID
SUBJECT
   NAME/DARDMAN, STAN D
   SEX/MALE    DATE OF BIRTH/10101950
   HEIGHT/510  EYE COLOR/GREEN
   ADDRESS/123 ANY STREET  CITY/MADISON  STATE/WISCONSIN  ZIP/53701
DETAIL
   SYSTEM IDENT #/22222
   LICENSE-CERTIFICATION #/1555
   ISSUE DATE/2011-11-01
   EXPIRATION DATE/2016-11-01
   ISSUING AGENCY/WI-DOJ
***** THIS INFORMATION MAY ONLY BE USED IN ACCORDANCE WITH WI STATUTE
      175.60(12) AND (12G).*****
```

New Plate Design for Firefighter/EMT Plates



Law enforcement should be aware of a new license plate design that is now being issued for firefighter and emergency medical technician license plates. The new license plate design is in addition to the existing designs.

Two license plates are issued, having black numbers and letters on a white background with a red border on the top and bottom of the plate. This is in contrast to the other possible plate design for these types of license plates, which have a strictly white background with no red border. On the left hand side of the plate will appear the red firefighter or blue emergency medical technician emblem. The word 'Wisconsin' will appear at the top of the plate and either the word(s) 'Firefighter' or 'Emergency Medical Technician' will appear at the bottom of the plate. Unless personalized, the plates will have five numbers followed by the stacked letters 'FF' or 'EM'. The change in plate design does not affect response format or license plate type code used for TIME System query (CV).

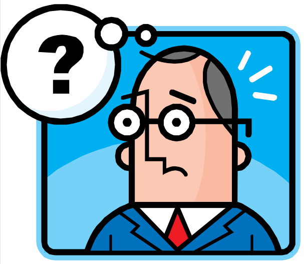
TIME & Technical Systems Manager

Courtney Doberstein joined the Crime Information Bureau on October 24th, 2011 as the TIME & Technical Systems Manager. Courtney comes from a communications center background and started her career in dispatch with the Germantown Police Department in 1997. She has also worked for the Sun Prairie Police Department and the Dane County 911 Public Safety Communications Center. Courtney served as a communications supervisor the last seven years at the Dane County 911 Public Safety Communications Center and is a NENA certified Emergency Number Professional (ENP). Courtney is very excited to be joining CIB and looks forward to continuing to serve the law enforcement community in this new role.

Social Services Access to TIME System Info

Reminder: Social Services agencies may have access to TIME System information in certain situations, provided they have obtained the required ORI. Be certain to use the social services agency's ORI when making TIME System queries on their behalf.

The Adam Walsh Child Protection and Safety Act of 2006 (Public law 109-248) provides access to the III and NCIC databases by governmental social service agencies with child protection responsibilities to be used only in investigating or responding to reports of child abuse, neglect, or exploitation. Agencies authorized this access are assigned an ORI number ending in the letter F. III/NCIC requests by these agencies must be performed using a social service "F" ORI and the purpose code "C". If the requesting agency does not have an ORI assigned, they should be instructed to contact CIB to have one assigned prior to providing them with TIME System data. Wisconsin and out-of-state criminal history requests may also be performed for these agencies, if requested, using their ORI. If another state rejects the request no information from that specific state should be provided to the requestor.



Help Eliminate Confusion

Have you ever sat in a class or attended a seminar and felt entirely lost? Dazed and confused, wondering what everyone is talking about? Most of us would agree this is an uncomfortable feeling. You can help prevent others from feeling this way.

While not a requirement, CIB highly recommends that prior to a student attending a TIME System basic certification class they take some time to familiarize themselves with the TIME/NCIC Systems and operations. The New Operator Handout was created for just such a purpose and is available on the CIB website, agencies should feel free to download, copy and distribute this handout to new system users.

Agencies are also reminded that users must achieve TIME System certification at the appropriate level within 6 months of employment or assignment as a terminal operator. As such, it is appropriate for a new user to access the system and run queries under the supervision of a certified operator to familiarize themselves with the system.

Use of Concealed Carry Information

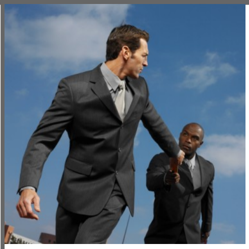
The concealed carry law is very specific in describing the limited occasions in which this information can be accessed and used. CIB encourages law enforcement officers and dispatchers to familiarize themselves with this information. The DOJ has compiled a list of frequently asked questions regarding the concealed carry law and made these questions and their answers available online. Two versions of these FAQ's exist. The public can find answers to their concealed carry questions on the DOJ website, http://www.doj.state.wi.us/dles/cib/ConcealedCarry/ConcealedCarry.asp. Another version of the FAQ's *dealing with issues specific to law enforcement* can be found on WILENET at https://wilenet.org/secure/html/ccw.htm. In addition, the Wisconsin Department of Natural Resources has compiled a list of DNR/hunting specific questions regarding the concealed carry law and made these questions and answers available on their website at http://dnr.wi.gov/org/es/enforcement/concealed_carry_q&a.htm. Some of the most common questions are excerpted here.

May law enforcement do random checks of citizens' CCW status; in the same manner they can gain driving status information by running license plates? No. Law enforcement can only check on CCW status after making an in person request to the subject. The Act only allows officers to check on the validity of the license presented to determine if the license is valid or if the individual does not have the card on his/her person, to confirm that the individual holds a valid license, or to investigate whether the person made false statements in the license application or renewal. 175.60 (12) (b) 1 and 2.

What can law enforcement do with CCW license information? Law enforcement can only use the information to confirm that a license or certification card is valid, or if the individual claims to have a license or a certification card but it is not in their possession, to check that the individual has a valid certification card or license, or to investigate whether a person made false statements in their license application or renewal. 175.60(12) A police officer who uses this information for purposes other than those described above, is subject to a criminal penalty of a fine of not more than $500, or imprisonment for not more than 30 days, or both. 175.60(17) (ag).

What are some of the things that law enforcement *cannot* do with certification or license information? Neither a law enforcement agency nor any of its employees may store or maintain information regarding an individual that was obtained from DOJ based on the individual's status as a licensee or certification card holder. Neither a law enforcement agency nor any of its employees may sort or access information regarding vehicle stops, investigations, civil or criminal offenses, or other activities involving the agency based on an individual's status as a licensee or holder of a certification card. 175.60(12) A police officer who violates this section is subject to a criminal penalty of a fine of not more than $500, or imprisonment for not more than 30 days or both. 175.60(17) (ag).

Can a law enforcement officer put on his report that he had contact with a subject and checked on his CCW license status? While the new statute places a premium on confidentiality, it would not seem to preclude placing this information on a report. However this report should not be flagged or separated in any way to highlight that a subject is a CCW license holder.



New NCIC Protective Interest File

NCIC has replaced the US Secret Service Protectee file with a new Protective Interest File (PIF). The PIF will now contain records entered by any law enforcement agency with a protective mission (as specified within municipal, state, or federal statutes, regulations, or other appropriate legal authority).

A record may be entered into the PIF for an individual for whom the authorized agency reasonably believes, based on its law enforcement investigation, may pose a threat to the physical safety of a protectee or their immediate family. A record entered into the PIF will assist agencies in determining the threatener's location and may provide the record owner with information related to the threatener's criminal activity.

Below is a sample response from the PIF, which is searched as part of a standard wanted person query. This is a sample record only, the warning caveat and instructions will differ depending on who the entering agency is, so be certain to review the entire record.

```
WARNING-DO NO ARREST OR DETAIN BASED SOLELY UPON THIS INFORMATION. OBTAIN IDENTIFYING
INFORMATION. SUBJECT IDENTIFIED AS A CREDIBLE THREATENER AND POTENTIAL DANGER TO U.S.
MARSHALS SERVICE PROTECTEE. IMMEDIATELY CONTACT USMS THREAT MANAGEMENT CENTER AT 202-
307-6100 FOR FURTHER INFORMATION.

MKE/POTENTIALLY DANGEROUS TO USMS PROTECTEE
VIOLENT TENDENCIES
ORI/MDUSM0123 NAM/SMITH, JOHN J SEX/M RAC/W POB/TX DOB/19511012
HGT/510 WGT/175 EYE/BRO HAI/BRO FBI/123456789 CTZ/US SKN/DRK
SMT/SC R HND
FPC/121011CO141159TTCI13 MNU/AS-123456789 SOC/123456789
OLN/11111111 OLS/MD OLY/199
DTT/20110803 OCA/123456273
MIS/KNOWN TO THREATEN FEDERAL COURT JUDGE
LIC/ABC123 LIS/MD LIY/2000 LIT/PC
IN/2Y27H5LI00009 VYR/1975
VMA/PONT VMO/VEN VST/2D VCO/BLU
ORI IS US MARSHALS SERVICE BALTIMORE FIELD OFFICE 301-307-6100
NIC/K146203706 DTE/20110804 DLU/20110804
*****CONTACT USMS THREAT MANAGEMENT CENTER AT 202-307-6100 WHICH HAS BEEN NOTIFIED OF
THIS TRANSACTION. THIS RECORD IS FOR CRIMINAL JUSTICE AGENCIES FOR CRIMINAL JUSTICE
PURPOSES.
***DO NOT DISSEMINATE OR USE FOR LICENSING AND EMPLOYMENT PURPOSES*****
```

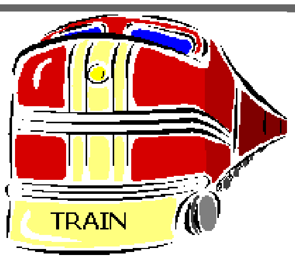
eTIME
Wisconsin Department of Justice
Crime Information Bureau

CCW and EBC

New TIME System transactions have been created in *eTIME* to allow law enforcement personnel to access the concealed carry database under circumstances authorized by the statutes to check the current status of a license. Act 35 is very specific about when law enforcement is authorized to access this information and the requirements for control of the data.

*e*TIME users will find new checkbox options titled "Concealed Carry Query" on the Person Search screen. Place a checkmark in this box if you wish to search the concealed carry databases of either Wisconsin or another state.

TRAIN Reports



CIB routinely receives calls from TRAIN agency administrators reporting having difficulty viewing and printing the reports available on TRAIN. Many times these difficulties could be avoided by ensuring the user's computer has been properly set-up to meet the requirements to use the TRAIN reporting feature.

Please refer to the Frequently Asked Questions link on the TRAIN login page for directions in setting up the report manager. There are numerous specific settings that must be enabled in order for reports to work properly. These settings may need to be configured in the Internet Zone, the Trusted Sites Zone, or both. Microsoft Office Web Components must also be installed on the computer in question.

Agencies should also be aware that TRAIN is not compatible with Internet Explorer 8 (IE8). Agencies that are using TRAIN in conjunction with IE8 do so at their own risk. Your agency may wish to consider using the Compatibility Mode to ensure proper performance. It is strongly recommended that you contact your local information technology staff before making any changes as they may determine that these options will interfere with other software your agency is using. While CIB staff will troubleshoot TRAIN issues to the best of their ability, as TRAIN does not support IE8 staff assistance in this area will be limited.

EBC No Record Responses

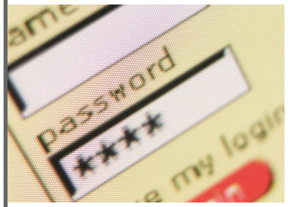
On occasion, CIB receives reports from *e*TIME browser client (EBC) users that they are receiving a 'no record exists' response that they believe to be in error.

This error message is typically seen when a user's internet browser does not routinely check for updated versions of the web page in question. Before reporting the problem to the TIME System Control Center, *e*TIME users are encouraged to try the following:

- Clear your internet browser's cache/delete browsing history. Location of this setting varies depending on the browser used, but it is typically found under the 'Tools-Internet Options-General' tab.
- Ensure your browser routinely checks for newer versions of stored pages. Again location of this setting varies, but it is typically found under the 'Tools-Internet Options-General-Browsing History Settings' tab. The preferred setting is 'every time I visit the webpage'.

DOT Information On WILENET

TIME System users may want to check out the Wisconsin Department of Transportation section of WILENET (once logged in, click on the 'Features' menu tab and then 'Department of Transportation'). Many DOT documents and manuals are readily available to law enforcement in this section, including the popular manual 'Interpreting Vehicle Registrations' which was recently updated.



Passwords: You Have the Power

Have you forgotten your password for TRAIN? eTIME? The Portal 100 software? WIJIS? : Users are reminded that when it comes to resetting a forgotten password, they have the power to do so. The following hints may come in handy:

- Your userid and password are the same for your TRAIN, eTIME, Portal 100 & WIJIS access. If you remember your password for one of these systems it is the same for the others.
- If you have forgotten your password, you can go to the TRAIN login page (https://ealogin.justice.wisconsin.gov) but *do not log in*. Instead click on the "forgot my password" link located to the right of the password field. You will be presented with your challenge question. Answer your challenge question correctly and you will be allowed to reset your password.
- If you have forgotten your password you could go to the *e*TIME login page (https://wi-time.gov) but *do not log in*. Instead click on the "forgot my password" link located above the userid field. You will be presented with anywhere from 1 – 3 challenge questions. Answer your challenge questions correctly and you will be allowed to reset your password.
- If you have forgotten your password, you could go to the WIJIS login page and click on the "Change Password" to reset your password.

Keep in mind that ***once you change your password in one of these applications it has been changed for the others as well,*** so if you change your password in TRAIN your password for Portal 100, eTIME, and WIJIS has been changed as well. If all else fails, and you are unable to reset your password by yourself or with the help of your agency's TRAIN administrator, you may call the TIME System Control Center (TSCC) 608-266-7633 to request your password be reset. You will need to confirm your identity to TSCC staff by providing a 4 digit PIN number. Once your identity has been verified staff will be able to process your password reset request.

Counterfeit Currency Case Guidelines

Due to some confusion that has been brought to the attention of the US Secret Service by some law enforcement agencies in Wisconsin regarding counterfeit current investigative and evidence procedures, the US Secret Service (USSS) has compiled the following guidelines to assist you. These guidelines are for use by Wisconsin law enforcement agencies when responding to and investigating counterfeit currency cases.

- Contact the USSS as soon as possible if there is a suspect or an arrest is made in a counterfeit case. The USSS can assist local law enforcement in determining whether currency is indeed counterfeit. In addition, the USSS can check the names of suspects to determine if they are on record with the USSS for prior counterfeiting activity or are involved in a current active USSS investigation. Office hours are Monday-Friday, 8AM-4:30PM, except federal holidays. During non-business hours law enforcement personnel can reach a USSS duty agent 24 hours/day, 7 days/week by calling the main USSS office number and dialing 0 when the answering machine picks up.

- Based on the information provided to the USSS, the local USSS duty agent may respond to an incident or agency location to assist in the investigation. If a suspect is arrested or detained, the USSS will make every effort to respond and interview the suspect immediately. Be aware that not all counterfeit currency cases become a federally prosecuted case. The USSS will assist in helping to and prosecute the case through an agency's respective district attorney's office if the case does not meet established federal prosecutorial guidelines. In some cases, the USSS may be unable to respond in a timely manner due to staffing constraints or travel distance. In all cases, please fax a copy of the incident report to the USSS as soon as possible.

- Counterfeit currency in evidence should be inventoried according to local law enforcement agency policy. The authority to confiscate counterfeit currency by the USSS, or to surrender counterfeit currency to the USSS, is derived from Title 18, United States Code, Section 492. In accordance with this law, the USSS Milwaukee and/or Madison offices must eventually receive all counterfeit currency recovered in Wisconsin. Counterfeit currency can remain in a local agency's evidence system as long as is necessary for an agency to conduct its investigation or adjudicate a case if it has been deemed that the case will not be prosecuted federally. At the conclusion of the investigation, or after the adjudication of a local case, the counterfeit currency must be sent to the USSS. Alternatively, in cases that are not being investigated or prosecuted on the state level, counterfeit currency must be sent to the USSS as soon as possible via the US Postal Service with a copy of the report attached. This is important so the counterfeit currency can be entered into the USSS counterfeit tracking system for accurate tracking of counterfeit currency activity. Under no circumstance should counterfeit currency be destroyed by a local law enforcement agency.

- The following counties are within the Secret Service Milwaukee Resident Office jurisdiction: Brown, Calumet, Dodge, Door, Florence, Fond Du Lac, Forest, Green Lake, Kenosha, Kewaunee, Langlade, Manitowoc, Marinette, Marquette, Menominee, Milwaukee, Oconto, Outagamie, Ozaukee, Racine, Shawano, Sheboygan, Walworth, Washington, Waukesha, Waupaca, Waushara, and Winnebago. If your agency is in one of the listed counties, please contact the Secret Service Milwaukee Resident Office at (414)297-3587, fax (414)297-3595, or mail the counterfeit currency to:

  U.S. Secret Service
  572 Federal Courthouse
  517 E. Wisconsin Avenue
  Milwaukee, WI 53202

  If your agency is within any other Wisconsin county not listed above, please contact the Secret Service Madison Resident agency at (608)264-5191, fax (608)264-5592, or mail the counterfeit currency to:

  U.S. Secret Service
  660 W. Washington Avenue, #305
  Madison, WI 53703

Should you have any questions on these guidelines or if the USSS can assist you in any way, please contact the Secret Service office that has jurisdiction in your respective county. Thank you for your continued support and assistance.

Contact Information

Agencies needing to contact NCIC, whether to request an offline search/message recall or to retrieve additional hits stored in a $B batch notification file are advised that while the NCIC ORI DCFBIWA00 remains functional, there is a new, preferred, faster method to contact NCIC. For requests such as those described, NCIC prefers the request be sent to the general email address of ioau@leo.gov.

State Wanted Query

The Portal 100 and *e*TIME browser software now include the ability for Wisconsin users to query another state's in-state warrants if that state supports these transactions. A query of the Nlets Help File, NLSWQHELP, will indicate which states participate.

Why would your agency care about these wanted person entries, as you can't take any enforcement action, since the warrants are non-extraditable?

While this information may not be valuable to an officer on a routine traffic stop, there are situations in which simply knowing the subject is wanted by an agency in another state may prove helpful to law enforcement personnel. For example, during criminal investigations or employment background checks it may be beneficial to law enforcement to know that outstanding warrants exist elsewhere. For example, an individual could be wanted in Michigan for the same offense they are being investigated for in Wisconsin, leading to contact between the two agencies proving beneficial to both.

Secure Areas and What is a Visitor?

As you may know, TIME System terminals must be placed to protect hardware, software and media. This would include workstations within your physically secure location. So what exactly is a physically secure location? According to the FBI, a physically secure location is a criminal justice facility, area, room, group of rooms within a criminal justice agency, or that are under the control of a criminal justice agency through a signed management control/security addendum agreement.

Restricted areas must be prominently posted and separated from non-restricted areas by physical barriers that restrict unauthorized access. Terminal monitors/displays must be positioned so the public/other unauthorized persons cannot view system information. Any access point to the restricted areas must be controlled or secured during both working and non-working hours, and an agency must verify an individual's access authorization before granting them access to a secure area. *Don't just assume because someone is in uniform they are authorized to access the secure area.* Visitors to the secure areas must be escorted at all times, and visitors must be authenticated before escorting them in the secure areas.

So who is a visitor subject to these requirements? *If the person has not completed the required background check and received security awareness training, they are considered a visitor. This would include officers from other departments.* If your agency wants to grant them unescorted access to your secure location, the required background check and security awareness training must be completed and your agency must add them to your authorized access list. The background check and security awareness training may be conducted by their employing agency, but before adding them to your authorized user list you must obtain verification these required steps have been completed.

Agencies must control physical access by authenticating visitors before authorizing escorted access to the physically secure location. The agency shall escort visitors at all times and monitor visitor activity. The agency must maintain visitor access records to the physically secure location that include name and agency of the visitor, form of identification, date of access, time of entry and departure, name and agency of person visited and visit purpose. These visitor access records should be frequently reviewed for accuracy and completeness, and the visitor access records shall be maintained for a minimum of one year.

System users should be aware of their surroundings and take steps to ensure unauthorized users do not access criminal justice information or the TIME/NCIC Systems. This may include challenging or questioning unescorted subjects, verifying credentials of strangers, and/or ensuring visitors and other unauthorized users are not ‘shoulder surfing’ (shoulder surfing refers to using direct observation techniques, such as looking over someone's shoulder, to get information). Numerous techniques and tools exist to help ensure the security of data. These may include the use of screensavers, screen shields, terminal location and positioning, etc. Each agency and user accessing the system is responsible for ensuring the security of the system and criminal justice information.

INTCH and WORCS

The Crime Information Bureau is replacing our current online record check system (INTCH – Internet Access to Criminal History). The new system, WORCS – Wisconsin Online Record Check System, is expected to be available around May 1, 2012.

While the online record check system is mainly used by non-law enforcement subjects requesting adult criminal history record information, the system is also used by law enforcement to review the results of applicant fingerprint based background checks sent to CIB, and is also used to generate invoices for billable criminal history requests (purpose code E or H).

The new WORCS program will streamline the invoicing process, creating electronic invoices that will be automatically emailed to your agency’s billing administrator. Emailing the invoices will save CIB thousands of dollars each month. In order for your agency to receive the invoices and fingerprint results you must take action to migrate your current account information from the old system into the new one before the new system goes into production.

Affected law enforcement agencies should have received a mailing from CIB containing account migration instructions. If you have questions about the new system or migration process, please contact Kevin Sime at simeka@doj.state.wi.us or 608-266-9398.

ALPR Extracts

The use of automated license plate recognition (ALPR) systems by Wisconsin law enforcement continues to grow. ALPR systems capture images of license plates using a camera typically mounted on a squad car. The images are sent to a computer interface, which then automatically searches the license plate numbers against a database - for example, a listing of stolen vehicles, felony vehicles, expired registrations, etc. If a match is made, the officer is alerted by an audible and visual signal, allowing him to take appropriate action.

So where does an agency get such a listing/database? Agencies that use automated license plate readers can get an extract from CIB of stolen vehicles, etc. listed in the CIB files, stolen vehicles, etc. listed in the NCIC files, and info from the DOT files on vehicles with expired/suspended plates, etc. These extracts are made available on the *e*TIME browser site. CIB now updates these extracts twice a day to ensure the most current information is available to law enforcement ALPR users. For further details, please contact TIME & *e*TIME Analyst Sara Phelan at phelansm@doj.state.wi.us or 608-266-7955.

Changes to IRP Vehicle Registration

The Wisconsin Department of Transportation implemented changes for those vehicles that have IRP (International Registration Plan) accounts, which refers to apportioned places for those motor carriers who travel interstate. The changes implement codes that will reflect the registration dates and IRP status clearly for all users.

When a plate query is run, and an apportioned plate is identified, the apportioned plate response will be included in the results. Not all apportioned plates will appear this way, you should continue to run apportioned plate queries directly using the appropriate plate type code. Sample responses appear below. Possible status codes appearing on the response may include the following:

- `==>>>>>LIY:01-02-2010 - EXPIRED <<<<==`
- `INSURANCE REQUIRED - NO VALID INSURANCE ON FILE`
- `CURRENT`
- `ASSUMED CURRENT`
- `IRP STATUS CODE INVALID`
- `FEDERAL OUT OF SERVICE`
- `NOT CURRENT`
- `ASSUMED NOT CURRENT`
- `EXPIRED`
- `NOT FOUND`
- `NO IRP STATUS FOUND`
- `NO IRP STATUS FOUND - PLEASE TRY AS A TK OR TL PLATE`

Questions contact DOT at 608-266-9900 or 608-261-2573

```
APO  Apportioned Plate Detail:
APO1   DONALD DUCKS TRUCKING INC
APO2   DBA: DONALD DUCKS TRUCKING INC
APO2a    1141 W MAIN ST
APO2d    DISNEY WORLD, WI 55555-941
APO3   OWNER: DONALD DUCKS TRUCKING INC
APO4   NBR: XXXXX / State: WI / Expiry: 04/30/2011
APO5   Year: 1906 / Make: PTRB / Weight: 180000
APO6   VIN: VIN1111111111111
APO7   Insurance status: Insured
APO7   IRP Status code: EXPIRED
APO8   WI Account: WI-XXXXXX
APO9   MC: XXXXXX
APO9   ICX: CCCC
APO9   LC: XXXXX

XXXXX/APO --- 1 of 1 --- 10-14-2011 12.33 PM CT
NAM:GOOFY TRANSPORTATION COMPANY
DBA:GOOFY TRANSPORTATION CO
STR:940 S DISNEY LAND CTY:DISNEY WORLD ST:WI ZIP:55555
OWN:DISNEY WORLD MASTER TITLING TRUST
LIC:XXXXX LST:WI
\
 ===>>>>> LIY:06-30-2011 - EXPIRED <<<<<===
/
VYR:2009 VMA:HINO VMA:HINO VIN:VIN33333333333333
INS_Sta:Insured
\
 ==>>> IRP STATUS CODE INVALID - NOT CURRENT <<<==
/
WI_Acct:WI-XXXXX INS_AUTH:XXXXXXX XXXXXXX
```

Certifications Error

Anyone who accesses the TIME System must have a current TIME System certification status. This is true whether a user is accessing via a full access TIME terminal or via the *e*TIME browser client (EBC). A user has six months to obtain an initial certification, and can access the system during this initial six month period. If a user's TIME System certification is expired, they should not be accessing the system until they are recertfied.

When an *e*TIME user logs in to *e*TIME and runs a query, the *e*TIME software automatically checks to see if the user's certification is current. If the user's certification has expired, they will not receive query results, but will instead receive an error message similar to the one below indicating that they are not certified to run the query in question.

Could not build CIB Vehicle Query transaction
[Error 5534] User CIBUSER1 is Not Certified to Run Requested Transaction

Could not build DOT Vehicle Registration Query transaction
[Error 5534] User CIBUSER1 is Not Certified to Run Requested Transaction

Could not build NCIC Vehicle Query transaction
[Error 5534] User CIBUSER1 is Not Certified to Run Requested Transaction

If You Don't Know Who You Are, We Don't Know Who You Are

Just a friendly reminder: when submitting fingerprints, please make sure your agency ORI is noted on the fingerprint card/submission. If no ORI appears, CIB is unable to identify who submitted the fingerprints and may be unable to process the fingerprint submission correctly.

Also, please be sure to provide the statute number and NCIC offense code for the violation submitted. Fingerprints submitted without complete charge information require CIB to contact the submitting agency to determine what the offense the subject was charged with, resulting in a delay in updating or establishing the subject's criminal history.

National Gang Intelligence Center

The FBI led National Gang Intelligence Center (NGIC) provides a web-based information system, NGIC Online, with tools for researching gang-related intelligence. After authenticating through the LEO website www.leo.gov users can connect directly to NGIC Online and access a variety of resources for gang-related intelligence, such as a gang encyclopedia, signs, symbols and tattoos database and the intelligence library. NGIC Online allows law enforcement to search the system's vast library of gang intelligence products/images, post announcements, access officer safety alerts, request information, and view the status of requests/submissions to the NGIC. Users also have the capability to solicit NGIC analytical assistance and communicate with national subject matter experts. NGIC Online also contains a gang investigations training and events calendar, as well as a discussion board. If you have any questions, contact the NGIC at NGIC@leo.gov or 1-800-366-9501

CIB
CRIME INFORMATION BUREAU

2012 CIB CONFERENCE

START PLANNING NOW

WEDNESDAY SEPTEMBER 19TH – FRIDAY SEPTEMBER 21ST, 2012
RADISSON HOTEL & CONFERENCE CENTER, GREEN BAY

National Center for Missing & Exploited Children

Heroin & Methamphetamines

Body snatchers-Michael Lock Case

Public CIB (Firearms Unit)

TIME System Interface/Security

Suicide Prevention in Law Enforcement

Justice Jeopardy

AFIS & CHRI

WSIC

TIME & eTIME Update

Ask CIB

More to come...

COMMENTS FROM PREVIOUS ATTENDEES:

"Always excellent information content"
"Great new ideas"
"Look forward to next year"

"Very good conference, put together well"
"Glad to see programs are being implemented"
"All DOJ classes are great as usual"

REGISTRATION WILL OPEN IN APRIL, FOR MORE INFORMATION PLEASE CHECK OUT THE WEBSITE: WWW.DOJ.STATE.WI.US/DLES/CIB/CONFERENCE.ASP

Important Interface Deadlines

The TIME Advisory Committee passed a motion at their April 2011 meeting requiring that all agencies become NCIC 2000 transaction compliant. The effective date will depend on whether your interface is query only or query and entry. Read on for the dates.

NCIC 2000 was an upgrade to transaction specifications by NCIC and included expanded fields and new transaction. The Wisconsin TIME System became NCIC 2000 compliant on February 13, 2005 by transforming non-NCIC 2000 transactions to NCIC 2000 formats before sending them to NCIC and creating a duplicate set of transactions with the NCIC 2000 formatting. Portal 100, Server to Server, and the eTIME Browser applications are all NCIC 2000 compliant.

NCIC 2000 compliance gives agencies the ability to enter additional information during record entry and impacts query results by allowing additional query fields. Recent TIME System enhancements have concentrated on NCIC 2000 compliant transactions. Example: Non-NCIC 2000 agencies cannot enter misdemeanor warrants in NCIC since they do not contain the EXL (extradition limitations field), a required field in NCIC 2000. NCIC 2000 transactions also include mandatory fields to ensure compliance with the CJIS security policy such as uniquely identifying each user. This is accomplished in the NCIC 2000 transactions with the required “OperatorID” Field.

The Advisory Policy Board (APB) voted in June 2011 to require the EXL Field for all warrant entries in NCIC. This field is defaulted behind the scene today for non-NCIC 2000 TIME System transactions but a required field for NCIC 2000 transactions. This change will require that all Wisconsin agencies transition to NCIC 2000 transactions for entries. The FBI CJIS Division is also beginning discussions for a rewrite of NCIC similar to what they did when they created NCIC 2000. Due to these changes and the benefits to local agencies the TIME Advisory Committee established the following dates to become NCIC 2000 transaction compliant in the TIME System.

- Effective January 1, 2012 - all new interfaces must use NCIC 2000 compliant transactions.
- Effective January 1, 2013 - all existing interfaces performing entry **and** query transactions must use NCIC 2000 compliant transactions.
- Effective January 1, 2015 – all existing interfaces performing query only transactions must use NCIC 2000 compliant transactions.

Due to limitations in the TIME System, interfaces must transition all transactions at the same time to NCIC 2000. The TIME System does not support a single interface with both non-NCIC 2000 and NCIC 2000 transactions. Please contact Chris Kalina at kalinaca@doj.state.wi.us to discuss transitioning your interface to NCIC 2000.

CIB
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	Vacant		608-267-1338	
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	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.statee.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	Kevin Sime	608-266-9398	608-267-4558	simeka@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