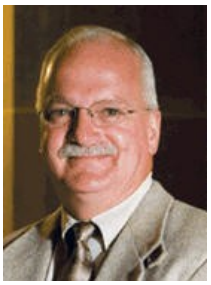
Wisconsin Department of Justice
Division of Law Enforcement Services

J. B. Van Hollen
Attorney General

TIME System Newsletter
Volume 2013-3
November 2013



The 2013 CIB Conference was held September 11th – 13th in Green Bay. From my perspective, it was a success in every way. A new attendance record was set for the conference which opened with a riveting overview of the Casey Anthony case presented by Major Ron Stucker of the Orange County Sheriff's Department. This was followed by a very informative and moving presentation by Chief Robert Paudert, retired, of the West Memphis Police Department. As always, each of you providing your thoughts and comments before, during, and after the conference contributed greatly to it's success. If you were unable to make the conference this year I hope to see you there next year.

The FBI CJIS Division released version 5.2 of the CJIS Security Policy effective August 9, 2013. There are some significant changes worth mentioning here. First, the requirement to maintain a visitor log was removed from the policy. This does not prevent an agency from continuing this practice as a department policy, and you are still required to control access to areas with CJIS data. This is accomplished by escorting unauthorized personnel and vetting authorized personnel through background checks, security awareness training and maintaining an authorized personnel list. Another significant change is the extension of the advanced authentication requirement from a police vehicle to September 30th, 2014 if you have not upgraded since 2005. The third significant change is the requirement that an agency have a local policy to validate a requestor of CJIS data as an authorized recipient. These topics are discussed in further detail within this newsletter.

INSIDE THIS ISSUE:

Locate	2
Nlets LPR	2
Reissued Plates	3
Portal 100	3
NCMEC SOTT	4
N-DEx	4
Validation	5
Advanced Auth.	5
Visitor Logs	5
Mgmt. Control	6
NCIC POIF	6
Nlets Help File	6
DOT Deceased	7
TRAIN Certificate	7
User Verification	7
Interface Deadline	8
Validate Users	8
Tablet Entry	8
Inmate Possession	9
TIME & Tablets	9

There are additional Security Policy changes being discussed that you should be aware of and will be hearing more about as they progress through the policy change process. The use of mobile / handheld type devices (i.e. smart phones and tablets) is growing each day. Not entirely unexpected, policy lags behind technology. Version 5.2 of the CJIS Security Policy begins to address the additional security requirements related to these types of devices by adding Section 5.5.7.3.3 Mobile Device Management (MDM). A pending policy change goes further by creating an entirely new section of the CJIS Security Policy, Section 5.13 Mobile Devices. You will be hearing more on this topic once it is fully vetted through the policy change process and approved by the FBI Director. Another pending change is the inclusion of a "police vehicle" as a physically secure location. Once this change is approved by the FBI Director and becomes policy the advanced authentication requirement from within a police vehicle will be postponed indefinitely. However, if your mobile device in the squad is used for TIME System inquires from outside the police vehicle, advanced authentication will still be required since it is no longer a secure location.

Walt Neverman

Walt Neverman
Director, Crime Information Bureau

Learn the Locate

The Locate procedure is becoming more common in Wisconsin, as NCIC requires a record to be in located status before detainer information can be added to a record. As such, a review of the Locate procedure is in order. The locate message adds information to a record indicating the subject or item has been found and provides details regarding locating agency, date, etc.

A Locate should be placed by the agency that *arrested or incarcerated* the subject, indicating that the subject is being detained. A Locate can only be placed **after** hit confirmation has occurred. Once the record has been located, the entering agency can then proceed with the existing transactions to enter the detainer.

An entering agency cannot place a Locate on their own record. If the arresting agency does not automatically place a Locate, the entering agency should make contact with the arresting agency and ask that they do so. As a last resort, if the arresting or incarcerating agency refuses to locate the record, the entering agency can request the TIME System Control Center (TSCC) to locate the record.

The purpose of a Locate is to indicate that the wanted person has been apprehended or stolen property has been located. A Locate message must be transmitted when an agency other than the originating agency of the record finds the missing person, apprehends the wanted person, or recovers the property on file in NCIC. It is recommended that a Locate be placed against a CIB record after hit confirmation has taken place. **Always** place a Locate after going through hit confirmation on an NCIC record.

In addition to its role in the NCIC detainer function, if the ORI fails to cancel the NCIC record, the Locate will purge it within five days. In the missing person file, a Locate immediately purges the record from the file. If a CIB record is being located, TSCC will contact the ORI and explain why the Locate is being placed and will advise the ORI that they have approximately 2 hours to cancel the record. If the ORI fails to cancel the record within the time allotted, TSCC will cancel the record.

LPR Info Available to TIME System Users

Agencies are discovering license plate reader (LPR) data can be useful for investigation as well as patrol. Nlets provides TIME System users with access to LPR data from the US Customs and Border Protection systems.

Because of the benefit of providing investigative information regarding stolen vehicles and other criminal activity, Customs and Border Protection provides data to the National Insurance Crime Bureau (NICB) from their license plate recognition systems installed at ports of entry between the US and Mexico and the US and Canada. Thanks to NICB and Customs and Border Patrol, this information is available to Nlets users.

Nlets users can run a special query to receive a list of when and where a vehicle has crossed the US border in the last 12 months. Not every border crossing has an LPR system installed. In addition, Nlets has partnered with National Vehicle Services and others to provide law enforcement agencies with access to a database of LPR data from *private* LPR systems, including parking garages, tollway systems, towing companies, etc. Transaction 0369 allows users to query these databases and is located in the 'NLETS/NCIC Special Messages' section of the Portal 100 menu.

License Plates Reissued

The Wisconsin Department of Transportation, Division of Motor Vehicles, began reissuing all sesquicentennial and remaining red letter auto plates on August 27, 2013. The process could cause confusion with customers who do not read the information sent with renewal and plate delivery. The reissuance will occur automatically when a registration renewal is completed on or after August 27, 2013 and will continue until all remaining Sesquicentennial and red letter standard auto plates are replaced which is anticipated to be in the fall of 2014.

Why is DMV doing this? These plates are years beyond their projected life cycle. Their reflectivity is decreased, and they are faded, making them less visible at night, and more difficult for law enforcement to read. In addition, the American Association of Motor Vehicle Administrators (AAMVA) recommends standards for license plate design: white backgrounds and black letters provide the best contrast and visibility.

Sesquicentennial plates will ***not*** be replaced with new Sesquicentennial plates, as they were a limited edition series created to commemorate the 150th anniversary of Wisconsin's 1848 statehood and were available from December 1996 through December 1998, at which time DMV's statutory authority to issue new Sesquicentennial plates ended. Depending on the type of registration for each vehicle, customers will receive *regular* auto, farm, light truck or motor home plates.

Customers may send plates back, or fail to understand *they do not have a choice* to replace their old plates.

If a customer has a personalized Sesquicentennial plate, they will receive regular plates with the same message. About 700 of these customers will not be able to retain their personalized plate message because it has already been issued more than once. DMV no longer allows any duplication of personalized plate messages due to law enforcement concerns. Affected customers may choose to reapply for a different personalized message or receive a regular sequentially numbered plate and will be notified in writing.

The DMV database is updated to show the new plate number. The vehicle owners have received the new registration but the old plate may still be on the vehicle. New year and month stickers will be sent with the new plates.

Portal 100 Compatibility

As agencies continue to update their computing environment, questions arise as to what operating system and browser the Portal 100 software is compatible with.

The most current version of the Portal 100 software is version 100.5.223. To check which version is installed, click on the 'HELP' (question mark) icon in the Portal 100 message window and choose 'ABOUT'. Portal 100 is compatible with Windows operating systems up to and including Windows 7© (32 bit version) and Internet Explorer 10 and below (those who use Internet Explorer 10 may need to use 'Compatibility Mode').

NCMEC SOTT

The Sex Offender Tracking Team (SOTT) at the National Center for Missing and Exploited Children (NCMEC) is available to offer technical assistance free of charge to federal, state, and local law enforcement agencies who are attempting to locate noncompliant sex offenders.

Members of the Sex Offender Tracking Team are also co-located at the US Marshals Service National Sex Offender Targeting Center (NSOTC). US Marshals personnel and other participating law enforcement agencies at the NSOTC can supply additional information that may be law enforcement sensitive.

Law enforcement can receive a comprehensive technical assistance report upon request from the NCMEC Sex Offender Tracking Team containing results found within several public records databases, NCIC (including NLETS/NCIC offline), as well as open source internet sites. As part of NCMEC, SOTT is also able to provide link analysis by comparing information found on sex offenders against NCMEC cases of missing children, child sexual exploitation, and attempted child abductions. Additional law enforcement sensitive searches can be requested and will be processed by the USMS personnel and other participating law enforcement agencies at the NSOTC.

Requests are entered and assigned to an analyst in the order they are received. All requests are entered as standard priority unless otherwise noted. Processing times vary based on the amount of requests currently in the queue. Please let SOTT know if your request is a high priority (results required within 48 hours or less) or if you have a target date or deadline for this request. SOTT will adjust the priority level to meet your needs.

Please send requests for Sex Offender Tracking Team assistance to email address NSOTC@NCMEC.org or call 1-800-THE-LOST (1-800-843-5678) and ask to speak with a Sex Offender Tracking Team analyst.

N-DEx

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.

Over 1,300 agencies nationwide contribute data to N-DEx, including federal agencies and entire state systems. Over 70 million records already exist in N-DEx. N-DEx is operational 24 x 7 and continues to grow in number of records and functionality.

One of the newest enhancements to N-DEx of interest to the law enforcement community is the acknowledgement that N-DEx information has value for more than just criminal investigations. N-DEx policy has changed, and law enforcement agencies are now allowed to search the N-DEx system when conducting background or pre-employment checks on prospective and current law enforcement employees.

Validation Reminders

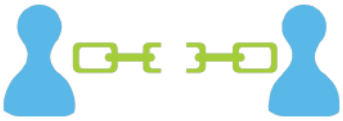
True or false: TIME System validation reminder notices are sent to all agencies.

Answer: false. While the initial email notification that a validation list is available is sent to all agencies with active records for that validation period, the validation reminder notices sent out via the TIME System at 20 days, 10 days and 1 day prior to the validation due date are only sent to agencies that have not yet completed their validation.

If your agency receives such a reminder it is because CIB records indicate you have not certified all records as having been validated, and should take action to do so. Remember to use the drop down feature of the 'Select File Type' field to see if records are listed for multiple file types.

Change to Advanced Authentication Deadline

For interim compliance with CJIS Security Policy, users accessing criminal justice information from devices associated with, and located within, a police vehicle are exempt from the advanced authentication requirement until *September 30th, 2014* if the information system being used has not been procured or upgraded anytime after September 30th, 2005. CJIS Security Policy defines a police vehicle as an enclosed criminal justice conveyance with the capability to comply, during operational periods, with Section 5.9.1.3.



Don't Click the Link

Many TIME System users have signed up for the Department of Justice's TIME System listserv to receive important TIME System broadcasts and information via email.

When the latest TIME System newsletter is published, an INFO broadcast will be sent via the TIME System directing users to the TIME newsletter page of WILENET. This broadcast is also sent to TIME System listserv users, who have discovered an issue.

When a listserv user clicks on the web address for the TIME newsletter page included in the broadcast/email, they receive an error message indicating "Page Not Found" and advising them to contact WILENET for assistance. However, there is a simple fix: type the web address into your browser using *all lower case characters* and you will be taken to the correct page.

Logs No Longer Needed

The requirement for keeping a log of visitors entering your agency's physically secure area has been removed from the NCIC Security Policy version 5.2 effective August 9, 2013.

Agencies are still required to control access to the secure area by authenticating visitors before granting escorted access, and must continue to escort visitors to the physically secure area and monitor visitor activity. Keeping a visitor log is still a good idea, but is no longer an NCIC requirement.

Signatures Needed: Management Control vs. Security Addendum

Agencies have contacted CIB with questions regarding the difference between the Management Control Agreement and the CJIS Security Addendum and under what situations each is needed.

A Management Control Agreement is required when a non-criminal justice agency is performing dispatch functions or a non-criminal justice agency hosts TIME System hardware (i.e. servers) outside the criminal justice agency's physically secure location. The management control agreement stipulates that management control of the criminal justice function remains solely with the criminal justice agency.

The CJIS Security Addendum is a uniform document which is included as part of an agreement between a government agency and a private contractor or vendor. The addendum provides information about the use, security and confidentiality of information obtained via the TIME/NCIC systems and also provides for sanctions in the event of a violation. All employees of the private contractor or vendor providing service to the criminal justice agency are required to read and sign the CJIS Security Addendum.

NCIC POIF Response Changes

Beginning August 4, 2013, TIME System users may have noticed slight changes to NCIC Protection Order/Injunction File responses.

NCIC POIF responses may now include information in 2 new fields: SVC (service information) and SVD (service date). The SVC field will indicate the status of the service of the order, and the SVD field will indicate the date the order was served. Both fields are optional. SVC may contain one of three possible values: 1 – served, 2 – not served or 3 – unknown.

In addition, there has been a change to one of the protection order conditions (PCO). The translation of PCO 07 has been changed to read "THE SUBJECT IS PROHIBITED FROM POSSESSING AND/OR PURCHASING A FIREARM OR OTHER WEAPONS AS IDENTIFIED IN THE MISCELLANEOUS FIELD." This change was made to reflect the fact that protection orders issued by some courts may prohibit the possession of other types of weapons, such as knives, bows, etc.

New NLETS Help File Lists Test Records

Nlets, the International Justice and Public Safety Network, has added another file to its list of Help files providing information to users.

A query of NLTSTHELP will provide users with a list of current test records for states which can be queried to view driver's license, vehicle registration, criminal history and other formats specific to states.

DOT Deceased Notation

Recently a user contacted CIB with an interesting question: "is it the responsibility of a law enforcement agency to notify the Department of Transportation of a subject's death?"

Each month, the DOT's Division of Motor Vehicles (DMV) updates its records with information received from the Department of Health Services Office of Vital Records. DMV receives a list of Wisconsin residents who have died in Wisconsin and a notation is put on the driving records of those people to prevent unlawful use of their driver's license or ID Card.

If you wish to provide notice of the death of a Wisconsin resident who died out-of-state, you may do so in writing to:

WisDOT-DIS
4802 Sheboygan Ave.
PO BOX 7983
Madison, WI 53707-7983

If you are in possession of the driver's license or ID card of someone who died, it is recommended that you destroy the card.

Certificates of Completion

Certificates of completion of TIME System training are available for printing from the TRAIN website. Upon successful completion of a class (online or instructor-led) users and/or their managers can log in to TRAIN to view and print a class completion certificate.

Navigate to the 'Learn' menu and choose the 'Training Schedule' option. Once a user's training schedule screen appears, change the view to show completed classes by using the drop down box in the center of the right hand side to select 'Completed Registrations'. Click on the name of the desired class, which is a hyperlink. Once the activity details screen appears, you should see a number of icons to the left of the class name. One of these icons looks like a certificate or diploma. Click on this icon, and the completion certificate will appear in a new window. Print the certificate as desired.

Who are You?

The phone rings at your department, and the caller states they are a clerk at the district attorney's office and asks that you run a criminal history query for them. Do you? How do you know they are who they say they are?

FBI CJIS Security Policy section 5.1.1 requires law enforcement agencies to have a local policy to validate that a requestor of criminal justice information is an authorized recipient before disseminating criminal justice information (such as only honoring requests that come through established channels/ procedures, confirming the requestor's identity in a secure manner, etc.). Make sure your agency has such policies/procedures in place to prevent the release of criminal justice information to unauthorized persons.

Important Interface Deadlines

Is your agency an interface agency? If so, read on. The TIME Advisory Committee passed a motion at their April 2011 meeting requiring that all agencies become NCIC 2000 transaction compliant. The effective date depends on whether your interface is query only or query and entry.

NCIC 2000 was an upgrade to transaction specifications by NCIC and included expanded fields and new transactions. Portal 100, Server to Server, and the *e*TIME Browser applications are all NCIC 2000 compliant.

Due to changes in NCIC requirements 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.

Validate Your List

Agencies are reminded that 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. Check to see if your agency's TRAIN roster lists only those who need TRAIN, TIME System or WIJIS access.

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.

Tablets

More and more tablet computers are purchased each day, and more and more tablet computers are reported stolen each day. The correct article type code for entry of a tablet computer into NCIC is DTABLET.

Possession of TIME System Materials

An agency recently contacted CIB with questions about a situation in which an inmate was found to be in possession of a copy of his Wisconsin criminal history record that appeared to have been obtained via the TIME System. The agency wanted to know if this was allowed.

CIB receives this type of question periodically. Whether or not the inmate is properly in possession of such a document depends on the circumstances under which they obtained it. There is no issue with an inmate possessing a copy of their Wisconsin criminal history record if it was obtained legally during the release of information to the defense during discovery under ss. 971.23 or if it was obtained as part of a request made under Wisconsin's open records law. These legal processes are covered by Wisconsin statute and are separate from TIME System policies. As always, agencies should consult their legal counsel if they have questions regarding these issues.

Tablets & the TIME System

The iPad. Galaxy Tab. Microsoft Surface. The Kindle. Tablet computers are becoming a part of daily life, and that includes becoming a part of the daily life of law enforcement.

TIME/NCIC System access using a tablet computer is currently allowed, provided the agency is able to meet all the technical requirements for wireless/mobile/cellular devices as outlined in the CJIS Security Policy. This includes such things as advanced authentication, encryption, firewalls, mobile device management and possibly more. Agencies have experimented with using the *e*TIME browser on such devices with limited success, which varies depending on operating system, browser used, and other factors. Agencies looking to access TIME/NCIC information via a tablet computer must ensure all applicable provisions of the FBI CJIS Security Policy are met, no matter what application or software they use to do so.

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	608-267-1338	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 Mgr.	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 Brad Rollo	608-264-6213 608-261-8134	608-264-6200 608-264-6200	lioneca@doj.state.wi.us rollobr@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