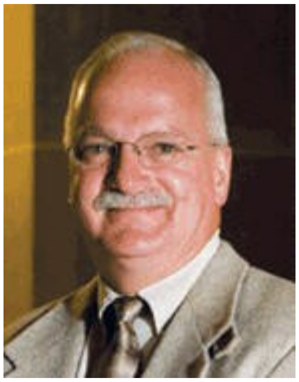
Wisconsin Department of Justice
Division of Law Enforcement Services

Brad D. Schimel
Attorney General

TIME System Newsletter
Volume 2018-2
June 2018

INSIDE THIS ISSUE:

The TIME System Newsletter continues to be our primary method of communicating TIME System information to our users. The Newsletter is posted on WILEnet along with TIME System Information messages and an email blast out to those of you that subscribed to TIME System Notifications in WILEnet. If you are not receiving these notices and want to subscribe please refer to page six of this Newsletter.



Please join me in congratulating Brad Rollo in his promotion to Deputy Director of CIB. Brad fills the vacancy created when Dennis Fortunato was promoted to fulfill the role as Director of Training and Standards.

I would like to thank everyone for your patience and cooperation as we worked through the online TIME System auditing process at the end of 2017. We were able to fine tune the process while completing our audit obligations for the 2015-2017 audit cycle. Audits for the next three year cycle (2018-2020) will be beginning soon. Wisconsin is scheduled to be audited by the FBI this year as we are every three years. Some of you may have been selected by the FBI to be audited as well. If your agency was selected, please feel free to contact CIB if we can be of any assistance as you prepare for their audit and the completion of the pre-audit questionnaires.

The Department of Justice has implemented the ability to send out a TIME System notification in the event of an Imminent Threat to Law Enforcement (ITLE). Hopefully this functionality is never needed but in the event it is, a message can be sent out to the ITLE destination on the TIME System, see page two of this Newsletter for more information on ITLE.

Cell phones have become something we depend upon each and every day. There are actually studies to determine if you are displaying symptoms of nomophobia, the fear of being without your mobile phone. Just imagine if your phone was stolen. The FBI recently conducted an analysis of stolen cell phones entered and found that many are entered incorrectly. This resulted in the issuance of a Best Practices for Entering Stolen Cell Phones guide that is available on WILEnet, see page 6 of this Newsletter for more information on this topic. Please ensure your agency is entering cell phones correctly for a quicker recovery and return to their owners.

Mark your calendars; based on feedback from last year's CIB Conference, it is returning to Green Bay for 2018. The 2018 CIB Conference is scheduled at the Radisson Hotel September 12th – 14th. Registration is open and available by logging into WILEnet, clicking on the Training Events menu item, selecting conferences, and scrolling down to September events. I look forward to seeing you at this year's conference.

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

New CIB Deputy Director

We would like to introduce the new Crime Information Bureau Deputy Director Brad Rollo. Brad has been with CIB since January 2012 when he started as a LTE in the Firearms Unit. He started during a very busy time in CIB with the implementation of concealed carry in Wisconsin. In May 2013, Brad's leadership abilities were recognized and he was promoted to a Justice Program Supervisor with oversight of the Firearms Unit. Brad received a Bachelor's Degree in Political Science in 2000 and a Master's Degree in Business Administration in 2004.

Imminent Threat to Law Enforcement

An individual in your jurisdiction is making threats to kill or seriously injure a law enforcement officer. You receive information that this suspect is headed toward a nearby county and you want to inform others of the threat. In Wisconsin, via the TIME System, an Imminent Threat to Law Enforcement (ITLE) administrative message can be broadcasted statewide to law enforcement only on a designated PSN. In the event of an imminent threat, the administrative message can be sent using the "ITLE" mnemonic. To have your agency added to the ITLE administrative message broadcast group, email cibpsn@doj.state.wi.us with your agency's name, telephone number, point of contact and PSN(s). If you do not know if your agency has already been added to the ITLE administrative message broadcast group, you can also request this information from the email above.

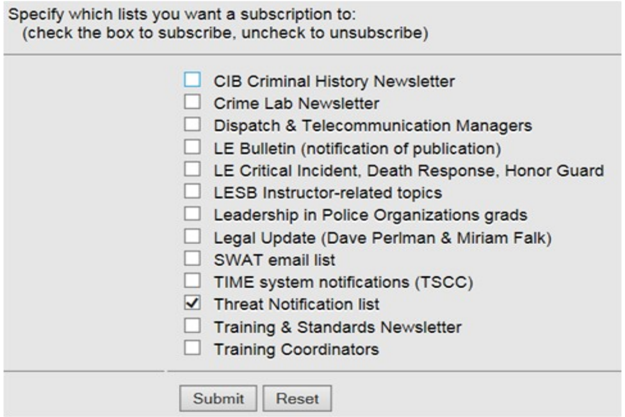
The following criteria must be met to qualify as an ITLE message:

1. Threat to cause death or serious injury to a law enforcement officer
2. Death or serious injury of a law enforcement officer in the line of duty; and/or
3. Law enforcement officer missing in connection with official duties

In addition to the administrative message, sworn law enforcement officers can also sign up for Imminent Threat emails. This email is transmitted by TSCC, via a listserv, once an ITLE message is sent.

To sign up complete the following steps:

1. Log into the secured side of WILEnet
2. Click on the "Training and Standards" tab
3. Click on "Email lists"
4. Click on "User profiles"
5. Select "Threat Notification list"
6. Click "Submit"



Specify which lists you want a subscription to:
(check the box to subscribe, uncheck to unsubscribe)

□ CIB Criminal History Newsletter
□ Crime Lab Newsletter
□ Dispatch & Telecommunication Managers
□ LE Bulletin (notification of publication)
□ LE Critical Incident, Death Response, Honor Guard
□ LESB Instructor-related topics
□ Leadership in Police Organizations grads
□ Legal Update (Dave Perlman & Miriam Falk)
□ SWAT email list
□ TIME system notifications (TSCC)
☑ Threat Notification list
□ Training & Standards Newsletter
□ Training Coordinators

Your decision to notify law enforcement around the state of an imminent threat could help save lives. CIB and the TIME System are proud to be able to offer this tool to help keep our law enforcement as safe as possible.

Drivers License vs. Identification Card vs. DOT-Issued Number

We regularly receive questions about how to properly use driver's license, identification card, and DOT-issued numbers (a number assigned by DOT to track citations when a driver's license or identification card has never been issued to the individual) when adding that information to a person record (e.g. warrant, protection order, missing person, etc.).

Due to the continued interest in this topic and the various TIME System requirements for entries, we thought a quick question and answer session may be helpful to you and your agency.

Q: You are preparing to enter a person record and find out the subject has a DOT-issued number but was never issued a driver's license or identification card…can you add this number to your entry?
A: No, DOT-issued numbers should not be listed in a TIME System entry, unless an actual card has been issued.

Q: I heard you can't enter an Identification Card into the TIME entry. Is this true?
A: Actually, you can enter the ID Card. If the individual has been issued a Wisconsin Department of Transportation (DOT) identification card, enter this number in the driver's license number field using the identification card year of expiration. If the identification card is a non-expiring identification card, indicate this in the miscellaneous or remarks field and *include in the miscellaneous or remarks field that the driver's license number is a Wisconsin identification card*.

If the individual has been issued a Wisconsin driver's license and a Wisconsin identification card and the operator uses the expiration date of the Wisconsin identification card, the operator must state in the miscellaneous or remarks field that the driver's license number is a Wisconsin identification card. An out-of-state ID card can be entered as a miscellaneous number.

Q: What if the subject has a non-expiring license or identification card?
A: If the license is non-expiring, use the code NX.

Q: My subject's driver's license is expired. Can I still use this license information?
A: If the Wisconsin driver's privileges are expired, revoked, canceled or suspended, the driver's license number can be entered using the date within the expiration date field. If no expiration date can be found, use UNKN in the expiration field.

The key to these and related questions is to determine if the subject has actually been issued the card. If so, you can use the information – even if it's expired. If the license/ID card number was generated by DOT computers but the subject never received an actual card you would not be able to use that information in your entry.

As always, contact cibtrain@doj.state.wi.us with any questions.

Mobile Device Security Considerations

Mobile devices which are able to view TIME/NCIC information are required to be secure and must meet the requirements of the FBI CJIS Security Policy. It is important to know the type of mobile device to best determine which policy areas apply to your agency mobile devices. Mobile devices can be categorized into two different classes: Full Featured Operating System (OS) devices and Limited Featured Operating System (OS) devices.

A full featured OS mobile device encompasses all laptop computers and some tablets. This includes "Toughbooks" and Surface Pro tablets. One piece that is usually characteristic of a full featured OS device is the keyboard requirement. Some will have permanently attached keyboards whereas others will come with detachable keyboards. Full featured OS devices will usually have its own built in security functions to include personal firewalls and a built in Wi-Fi modem.

Limited featured OS devices encompass all smart phones and most tablets. Some smaller laptop devices such as Chrome books qualify as they do not run on a full featured OS and usually require you to download or install certain applications which normally would come built in with a full featured OS computer. Their hardware is also usually not as fast or powerful as larger full featured OS devices and lack the storage space a full featured OS system normally has. Most limited featured OS devices run on either Android or Apple based software depending on the brand of the device. Some of these devices will have their own firewalls and security features, although the majority of the devices are not as secure as a full featured OS system would be.

Every mobile device that can access and/or store Criminal Justice Information (CJI) and is not locked in a secure area or squad car must have two factor advanced authentication implemented. Every limited featured OS device is required to have a Mobile Data Management (MDM) program installed so that the agency can protect the device if lost or stolen, and if necessary remotely wipe/sanitize the device. All mobile device security requirements are listed in the CJIS Security Policy which is available for online from the FBI CJIS Division at the following link: https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center.

CJIS Information letters can be found on WILEnet at the following link: https://wilenet.org/html/cib/news-fbi/index.htm

Validation Officers must certify canceled records to complete the validation process.

Law Enforcement Officer Flying Armed

Law enforcement agencies have the ability to send officers on flights while armed in connection with official duties. Transportation Safety Administration (TSA) requires that all law enforcement officers flying armed submit officer and flight information to the Federal Air Marshal Service. The Federal Air Marshal Service will return a unique alphanumeric identifier that will be used by the officer when checking in at the airport.

The Crime Information Bureau has updated the form that will allow law enforcement agencies to send officer and flight information to the Federal Air Marshal Service through Nlets. Certain information must be transmitted in order to receive an approval number from the Federal Air Marshal Service. These updates provide more detailed information regarding the reason for travel and allow the user to enter multiple connecting flights into one request.

Before submitting the request, the law enforcement agency must have already bought the airline ticket(s) in the name of the law enforcement officer(s). A complete request must be submitted for each direction of travel during the journey. For example, if an officer is flying from Milwaukee to Richmond, VA with a connecting flight in Atlanta, GA, two LEOFA submissions would be needed: one for the flights to Richmond, another for the flights back to Wisconsin. In Portal100, form 0443 will be used to submit the request. When completing the form, the following information is required:

Officer's name (last name, first name)

- Agency
- Officer badge number
- Officer type (state or local agency officer)
- Name of authorizing official (this is the Chief, Sheriff or Law Enforcement Agency Administrator who endorses and approves the submission of the LEOFA request)
- Officer and Agency phone numbers
- Explanation of individual travel (must be one word-no space-to explain the reason why the officer must be armed: PROTECTIVEDETAIL, PRISONER, INVESTIGATION, etc.)
- Name of escorted individual (example is a prisoner transport; if not escorting a person, leave blank or use NA)
- Airline name
- Flight number (all flight numbers in one direction to final destination)
- Flight date
- Airport abbreviations for departing connecting and final destinations

CIB has new PSN request forms available at: https://wilenet.org/html/cib/manuals-forms/non-training-forms/psn-request-form.pdf

If there is a mistake made during the entry and it is not caught until after the form is submitted, the person submitting the form should simply submit a new form with the corrected information.

For more information or to request training materials, visit the TSA website at https://www.tsa.gov/travel/law-enforcement.

Importance of Test Data

It is very important that users are using test data located on WILEnet when testing the TIME System. Always refrain from testing with your own information or anyone that you may know as this is in violation of the CJIS Security Policy. Not only is this against policy, but also can lead to unfortunate circumstances. For example: do not enter your own personal vehicle as a stolen vehicle. Another example is while testing your agency's live-scan, never submit your personal finger prints because the arrest entered will remain on your criminal record and could prevent you from obtaining additional clearances or even employment. The test data provided by CIB returns information that is known and expected, unlike running yourself or others, you may not receive anything in return that will ensure the testing was successful.

State Patrol STOC (Statewide Traffic Operations Center) now goes by the name of TMC (Traffic Management Center). WTMC is the mnemonic for administrative messages.

How to Find Newsletter Articles

Have you ever wondered how to find out if there is a newsletter article on a topic? When a new functionality exists in the TIME System, the topic is covered in the TIME System Newsletter. The newsletters are posted on WILEnet at the following link: https://wilenet.org/html/cib/news-time/index.htm. An index also exists on this link for a key word search of the past newsletters posted on WILEnet.

When CIB releases a new version of the TIME System Newsletter, a broadcast message is sent out over the TIME System to advise agency personnel that it is available on WILEnet. You can also sign up to be notified when a new edition is posted to WILEnet, by subscribing to the TIME System notifications. (see page 2 of this newsletter in the article titled, Imminent Threat to Law Enforcement, for detailed instructions for Email notifications)

Cell Phone Entries in the TIME System

In the November 20, 2017 CJIS Information letter, posted on WILEnet at the following link: https://wilenet.org/html/cib/news-fbi/11-2017.pdf, there is an article titled, Best Practices for Entering Stolen Cell Phones into the Article File of the National Crime Information Center. NCIC staff identified cell phones and other articles that were improperly entered and conveyed this information to CIB. CIB has contacted those agencies with article files that were improperly entered.

Stolen Cell/Smart phones should be entered with the type code DCELLPH. While DCELLPH does not appear in the Portal 100 type code table, the type code can be entered as DCELLPH. DCELLPH will be included in the next Portal 100 Service Pack.

CIB Contacts

	Name	Telephone	Fax Number	Email
Director	Walt Neverman	608-264-6207	608-267-1338	nevermanwm@doj.state.wi.us
Deputy Director	Bradley Rollo	608-261-8134	608-267-1338	rollobr@doj.state.wi.us
TIME & Technical Services Manager	Courtney Doberstein	608-266-0872	608-267-1338	dobersteincl@doj.state.wi.us
Training Officer - Senior	Susan Whitstone	608-266-9341	608-267-1338	whitstonese@doj.state.wi.us
Training Officer	Emily Freshcorn	608-261-5800	608-267-1338	freshcornek@doj.state.wi.us
Training Officer	Gregory Kosharek	608-261-7667	608-267-1338	kosharekgr@doj.state.wi.us
TIME System Operations Manager	Chris Kalina	608-266-7394	608-267-1338	kalinaca@doj.state.wi.us
TIME & *e*TIME	Mary Moroney	608-266-2426	608-267-1338	moroneym@doj.state.wi.us
TIME & *e*TIME, Validation, Livescan Analyst	Sarah Steindorf	608-261-8135	608-267-1338	steindorfsr@doj.state.wi.us
TIME & *e*TIME, Validation, Livescan Analyst	Craig Thering	608-266-7792	608-267-1338	theringcd@doj.state.wi.us
TIME & *e*TIME, Validation, Livescan Analyst	Zach Polachek	608-264-9470	608-266-6924	polachekzd@doj.state.wi.us
TIME & *e*TIME	John Ide	608-264-9490	608-267-1338	idejh@doj.state.wi.us
TIME System Audits			608-267-1338	cibaudit@doj.state.wi.us
TIME Billing			608-267-1338	timebilling@doj.state.wi.us
AFIS Operations Manager	Adrianna Bast	414-382-7500	414-382-7507	bastar@doj.state.wi.us
Criminal History Section (Record Check & Criminal Records) Supplies and Imaging	Katie Schuh	608-266-0335	608-267-4558	schuhkr@doj.state.wi.us
	Jon Morrison	608-261-6267	608-267-4558	morrisonjd@doj.state.wi.us
Firearms Unit	Andrew Nowlan	608-267-2776	608-267-1338	nowlanam@doj.state.wi.us
	Vacant		608-267-1338	
TRAIN		608-266-7792	608-267-1338	cibtrain@doj.state.wi.us
WIJIS Justice Gateway	Zach Polachek	608-264-9470	608-266-6924	wijis@doj.state.wi.us
TSCC		608-266-7633	608-266-7315	
WILEnet		608-266-8800		wilenet@doj.state.wi.us

Check the WILEnet website for additional data at www.wilenet.org