WISCONSIN DEPARTMENT OF JUSTICE
DIVISION OF LAW ENFORCEMENT SERVICES

J.B. VAN HOLLEN
ATTORNEY GENERAL

VOLUME 2009-1
JANUARY 2009

TIME System Newsletter
Crime Information Bureau

Hello!

Effective October 13, 2008, I was appointed Director of the Crime Information Bureau for the Wisconsin Department of Justice (DOJ) by Attorney General J.B. Van Hollen. I have held several positions within the Department of Justice including Training Officer, TIME System Operations Coordinator, Field Services Supervisor and most recently the TIME & Technical Services Manager. I began my career with the State of Wisconsin as a Police Communications Operator for the Wisconsin State Patrol and also worked as a Regulation Compliance Investigator with the Department of Regulation & Licensing before coming to DOJ.

Would this article have been the same without the image?

For many of you that I have met over the years, your mind would have used an image from the past and for others your mind would have created a mental picture based on what information you know about me. This may or may not have been an accurate image of me.

We are currently working on and planning several projects that will bring images to the TIME System. This will include: images entered by local agencies for person and vehicle records stored in NCIC, out-of-state driver images from those states that have implemented and allow this sharing, and electronic mug shots submitted with electronic arrest fingerprint cards. A picture may not always be worth a thousand words but when an officer is attempting to identify a subject on the street, it will speak loudly. Of course the image must come from a source you know and trust. These images will be those that you have collected along with DMV photos from other states.

I look forward to working with you to continue improving the TIME System to meet your needs. Please feel free to contact me or any of the CIB staff with your ideas and suggestions.

Walt Neverman
Director CIB

INSIDE THIS ISSUE:

Validation Reminder

Agencies are reminded that due to the limited time which the CIB has to validate files with NCIC, IF CERTIFICATION OF VALIDATION IS NOT RECEIVED BY THE DATE INDICATED, WE WILL HAVE NO ALTERNATIVE BUT TO PURGE ALL THE RECORDS FOR THAT MONTH.

In recent months, numerous agencies have failed to certify that their records have been validated, despite numerous warning messages and phone calls. Reminder messages are only sent to agencies whose certification is *still outstanding*, so if your agency receives a reminder message it means CIB has not received your certification.

Online validation users should know that they must certify *every* record listed as validated. If an online validation agency cancels a record, they still must mark it as having been validated or their validation will be considered incomplete.

Are records really purged if validation certification is not received? Yes. An agency recently had nearly 50 wanted person, gun, vehicle, and other records removed from the system when their certification letter was not received in a timely manner – and they were not the only agency that had records purged in this validation period. Not only is this a serious liability risk for the agency, but such a situation causes additional work, as agencies have to locate case files and re-enter records as appropriate. Don't let this happen to you.

Interpol Agreement

The Wisconsin Department of Justice recently signed an agreement with INTERPOL, the International Criminal Police Organization, that provides access via NLETS to INTERPOL wanted person, travel document, and vehicle databases.

New query transactions are available in the Portal 100 software under the 'NLETS/NCIC Special Messages' section of the menu. Before agencies may use these transactions, they must sign a special Interpol Agreement that contains specific restrictions regarding Interpol information.

Agency administrators may send an email requesting access to Interpol information to cibtrain@doj.state.wi.us. Please indicate in the email which workstations/PSN's will need this authority. A copy of the required agreement will be sent to your agency for signature. Once CIB has received the signed agreement, the needed changes to your PSN's will be made and you will be notified when the changes have been completed.

Sheriff's departments, communications centers, and others that provide dispatch service and/or TIME System access for other agencies should be aware that each department they provide services for must sign the required agreement before access will be granted to the providing agency.

For more detailed information regarding these Interpol queries, please see related article in the September 2008 TIME System newsletter.

TIME System Users, Do You Know Your Purpose?

As TIME System users should know, when requesting criminal history record information, a user is required to specify 'why' the information is being requested by choosing the appropriate purpose code: C, D, E, F, H or J. The use of criminal history record information is regulated by state and federal law, and use of the correct purpose code ensures only the proper information is returned.

In the last TIME newsletter, we reviewed the proper use of purpose code E. In this newsletter, please take a moment to review the use of purpose code C, the most commonly used purpose code.

Purpose code C is used for criminal justice/law enforcement purposes. In other words, it is used for official duties in connection with administration of criminal justice. ("Administration of criminal justice" is defined as the performance of any of the following activities: detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision or rehabilitation of accused persons or criminal offenders.) Purpose code C is accepted at both the state and federal (III) level, and will return information on both adult and juvenile records.

A law enforcement agency may also request a criminal history record check using purpose code C for the security of the criminal justice facility; for example:

- Vendors or contractors at the criminal justice agency who are *not* involved with the actual administration of criminal justice at the criminal justice agency; e.g. janitors, cooks individuals responsible for maintaining vending machines, etc.
- Volunteers at the criminal justice agency who are *not* involved with the actual administration of criminal justice; e.g., participants in ride along programs, volunteers at a confinement facility who are providing social/community services.
- Confinement facility visitors.
- Inmates of a confinement facility.
- Inmate mail. A prisoner's list of names and addresses of those wishing to correspond with the prisoner. A criminal history records check may be used when there is reason to believe that criminal activity is occurring or has occurred.

*e*TIME Timer

Beginning in May 2008, in addition to inputting user name and password, users may now indicate on the WILENET login screen whether or not they are logging in from a secure location (law enforcement agency or squad). If the user indicates they are logging in from a secure location, the WILENET and *e*TIME inactivity timer will be extended to 4 hours from the current 30 minutes.

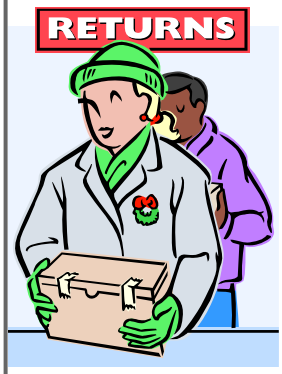
*e*TIME Browser users are reminded, however, that their department computer network or internet service provider may have a more restrictive timer setting, causing their *e*TIME session to end before the 4 hour inactivity time established by CIB. If your *e*TIME sessions are ending prematurely, you should check with your IT professional to determine if an internal or network timer is the cause.

Interstate Identification Index

As of October 5, 2008, all 50 states and the District of Columbia are Interstate Identification Index (III) participants, and as such, provide electronic access to their criminal history records. FBI staff continue to work with US territories to becomes III participants, and 2 (Guam and American Samoa) have taken the first steps toward participation.

III is an automated index on persons with criminal records. III provides access to FBI identification segments and criminal records. A single agency in each state is responsible for providing the state's records. Criminal justice agencies can use this information for law enforcement purposes; e.g. criminal investigations, bond setting, charging determinations, sentencing and criminal justice employment**. Criminal records obtained through III cannot be used for licensing or employment purposes.**

The III index points to the criminal history record residing either in the FBI or the particular state(s) holding the information. An initial query of III is made to determine the existence of a record. The FBI computer searches its database and returns a list of possible ident segments relating to your request. The segments contain physical identifiers, additional numeric data and aliases. Upon determining a segment is related to the person in question, a second transaction is necessary to obtain the criminal record. The ident segment will indicate the location of the record and how to access it.



Save Yourself a Send-Back

CIB has been receiving some MDC exams that do not include the name of the individual who provided the MDC classroom training. Without this information we are not able to determine that the training was provided by an authorized Agency Assigned Instructor (AAI). Failure to provide the name of the AAI administering the training will now result in the exam being sent back to the agency, with no credit given for the exam results. MDC materials submitted to CIB must also include the student's *complete* name as it appears in the TRAIN database. This information must be legible. With over 23,000 active TIME System users, if a complete, legible name is not included, CIB is unable to add the MDC information to the database, and materials may be returned to the agency for clarification.

Each year the CIB training staff updates the training handouts and related materials. The most current handouts and exam materials are located on the CIB website www.doj.state.wi.us/dles/cib. AAI's should check the website for new 2009 materials to ensure they are providing the most current information to their users, and are also providing CIB with the necessary information.

Latest License Plates

TIME System users should be aware of 2 new Wisconsin license plate types being issued by the Department of Transportation (DOT). Donate Life Wisconsin plates are issued to anyone interested in expressing support for organ, tissue and eye donation. The plates have a white background with black lettering. The Donate Life symbol, a green & blue square with the words "Donate Life" is on the left.

"Wisconsin" is printed at the top and "Organ, Tissue & Eye" is printed at the bottom of the plates in red letters. Non-personalized Donate Life plates have the letter 'S' as a suffix.

Civil Air Patrol license plates are available only to persons who are current or retired members of the Civil Air Patrol, a non-profit organization which is an auxiliary of the US Air Force. The plates have a white background with black lettering. The Civil Air Patrol logo (blue shield) is on the left. "Wisconsin" is printed at the top and "Civil Air Patrol" is printed at the bottom of the plates in red letters. Non-personalized Civil Air Patrol plates have the letter 'R' as a suffix.

Both new plate types may be queried on the TIME System using the 'CV" license plate code. For TIME System entries, license plate type code 'ZZ' should be used.

New License Plate Design

Heavy vehicle plates renewed after October 31, 2008 will be issued new license plates. The new plates have a grey background with black lettering. There may be a short period of time after the renewal of the registration where the new plate number will be shown on DMV records even though the old plate is still on the vehicle. Heavy vehicle plates issued after December 1, 2008 will also receive the new plate design. Questions can be directed to the registration & title hotline.

The heavy vehicle plates being reissued include:

- Farm Trailer
- Heavy Farm Truck (over 12000 lbs)
- Heavy Trailer (over 3000 lbs)
- Heavy Truck (over 8000 lbs)
- Tractor

Printer Possibilities

As TIME System agencies may know, the standard printer for use with the Portal 100 software is an Okidata dot matrix printer, in fact, for agencies who are part of the state maintenance contract, this is the only printer supported. While an Okidata dot matrix printer is the standard, supported printer, agencies are successfully using other types of printers, including laser and ink jet printers, to print TIME System responses.

Agencies have reported some success with several HP models, including the HP 1200, HP 1320, and HP 2300. Agencies have also reported success with Okidata laser printers, including model B4350. It has also been reported that the printer needs to have an Epson or Okidata emulation setting available.

CIB does not endorse any particular printer other than the standard Okidata dot matrix for use with the Portal 100 software, but is passing on this information. Agencies wishing to use other printers to print TIME System responses should perform their own research and testing to ensure the chosen printer meets their needs.

Search Stolen Property

Investigators may not be aware of other investigative resources that are available for use when trying to locate stolen property, and may wish to check the internet. Various websites provide online registries of stolen property. These sites may include information from law enforcement, the general public, auction houses, dealers, insurers, and pawnbrokers, Consumers can check a purchase before they buy; while pawnshops and secondhand retailers can check items they suspect are stolen.

Typically, the online record includes information needed to identify an item, the police agency that took the report, and additional information. To identify investigatory leads, the website may require users to register before performing a search. Then, if a searcher gets an exact match on an item, the police may be sent an alert with the searcher's name, address, e-mail, telephone number, etc.

Law enforcement may find information from such sites valuable, as they may contain information unavailable via traditional law enforcement databases such as NCIC. These online sources may contain information on stolen property that does not qualify for entry into NCIC or state databases, and information on stolen property from other countries may be available as well. One such site boasts their database has over 650,000 items from the UK and Europe.

There are numerous such sites available. To find them, simply type "stolen property search" or a similar phrase into your favorite search engine, and begin to reap another benefit of the Internet.

TB or Not TB, That is the Question

TIME System users may find a Wisconsin Department of Transportation enhancement to be helpful. License plate type code TB (Tribal) may now be used when querying a tribal license plate via WI DOT. When a tribal license plate is queried using this code vehicle owner information will be returned, however responses will not include license plate expiration or vehicle description information.

Registration information for tribal license plates may be obtained by contacting the individual tribe's licensing coordinator during business hours. If the vehicle identification number is queried via the TIME System basic registration information will be returned, however responses will not include expiration date or license plate information.

License plates are issued by the Wisconsin Indian tribes and bands to members and non-members who reside on the reservation. Four Indian Nations located in Wisconsin have issued their own tribal license plates: the Menominee Indian Nation, the Lac Du Flambeau Band of Lake Superior Chippewa, the Oneida Tribe of Indians of Wisconsin and the Bad River Band of Lake Superior Chippewa.

'B' Careful of Illinois 'B' Trucks

TIME System users should be aware of potential problems when querying Illinois 'B' light truck license plates.

In order to receive a valid registration response, the license plate query must be sent in a specific format. A hyphen (-) followed by the letter 'B 'must be included for the Illinois Department of Motor Vehicles to process the query and locate the correct registration information. For example, Illinois light truck license plate 12345A would be queried as 12345A-B.

This use of a special character by Illinois causes some difficulties for TIME System users. First of all, NCIC does not allow the use of the hyphen in the license plate field. This means a query that includes the hyphen character will be rejected by NCIC and will *not be searched* against NCIC's stolen vehicle file. A second query of the license plate is required, omitting the hyphen, to check for nationwide stolen status.

Second, some older software, such as Enforcer, does not allow the use of a hyphen in the license plate field. Agencies in this situation will have to contact the Illinois DMV directly to obtain needed registration information for Illinois 'B' truck plates. These agencies should also explore upgrading their software to allow for this and other TIME System changes.

DOT Dilemma

TIME System and *e*TIME browser users have recently reported an issue with Wisconsin Department of Transportation (DOT) driver responses. In some cases agencies have discovered information on a driver's license response varies depending on whether the information was requested using the *e*TIME browser or a traditional TIME System terminal.

Driver's license responses received via the TIME System and *e*TIME browser come directly from WI DOT databases, the TIME System does not change the data. DOT maintains 2 separate databases of driver's license information. Driver's license responses received via the *e*TIME browser come from one DOT database (DB2), while driver's license responses received via a traditional TIME System terminal come from the other DOT database (FH). In theory, information in both databases is supposed to be identical, however several recent cases have shown the information may not be the same.

For example, address information may differ. The most current address information will be available on the *e*TIME browser response. A TIME inquiry will provide the current address associated with a subject's **driver license or ID**. An *e*TIME inquiry is linked to a shared customer database, and can be updated by registration products (e.g. license plate) and/or driver products (driver license, ID card). Address information can get out of sync when a customer updates address information on a vehicle registration. This may cause the address returned in the *e*TIME browser to be different than the traditional TIME System. *e*TIME will provide the most current address from the DOT shared customer database.

Agencies are urged to use caution and verify DOT driver's license data directly with DOT when a discrepancy between responses is noted.

Foreign Nationals

Dealing with foreign nationals presents challenges and obligations for law enforcement. There are a myriad of requirements and issues that may arise when law enforcement deals with foreign nationals.

In addition to a multitude of other information, when querying a person, TIME System users may receive responses from the NCIC Immigration Violators File (IVF). The following information regarding responses from the IVF is reprinted from the Wisconsin Department of Justice "Guide for Contact with Foreign Nationals". The guide is available on WILENET in the 'Legal Drawer' section listed under 'Resources' and contains additional information of value to law enforcement, including information regarding dealing with subjects claiming diplomatic immunity and information regarding required consular notification of detained subjects. Check it out!

Dealing with NCIC information about Foreign Nationals

Once the officer has done a TIME System check on a lawfully stopped person the officer may discover that the subject has a criminal or civil immigration violation status. There are three primary IVF categories entered into NCIC. These three categories are 1) Deported Felon 2) Absconder, and 3) NSEERS. The procedure to follow differs depending on which kind of violation is involved.

Criminal Immigration Violation (Deported Felon, Absconder)
Wisconsin law enforcement officers have the legal authority to enforce federal criminal immigration status violations. Criminal immigration violations include absconders and deported felons. Consequently, Wisconsin law enforcement officers may arrest subjects whose NCIC report show that the subject has federal criminal immigration status violations. Before doing so, however, law enforcement must check with the Immigration/Customs Enforcement (ICE) Law Enforcement Support center (LESC) to confirm the "hit" from NCIC. Of course, the officer may arrest the subject for any criminal violation under Wisconsin law regardless of the subject's immigration status.

Civil Immigration Violation (NSEERS)
Wisconsin law enforcement officers do not have the legal authority to enforce federal civil immigration status violations. Civil immigration violations include being illegally present in the United States and failure to depart after the expiration of a visa. Accordingly, if the NCIC check shows the subject to be an illegal alien, a "hit" for the NSEERS category, this is not sufficient in and of itself to justify further detention or an arrest. After the subject is released there is nothing to compel or to prohibit law enforcement from reporting the offender to ICE. The Wisconsin Attorney General recommends, however, that law enforcement report such offenders to Immigration/Customs Enforcement (ICE) or to the Wisconsin State Intelligence Center (WSIC), which will report the offenders to ICE. However, the officer may detain or arrest the subject for suspected violations of Wisconsin law.

Notification if there is a "hit" on person arrested for some violation of Wisconsin law
If an individual is arrested or detained based on an independent legal basis under Wisconsin law, and an NCIC "hit" indicates an NSEERS violation, or the individual's immigration status is questioned, the LESC may be contacted. Thus, while state law enforcement does not have the authority to arrest based on civil immigration violations, they may contact the LESC if the individual is otherwise lawfully detained.

Key Points:

- NCIC has three categories of immigration violations: Deported Felon, Absconders, or NSEERS
- Wisconsin law enforcement can enforce criminal immigration status violations - Deported Felon or Absconder categories. However before arresting, the subject law enforcement should confirm the "hit" from NCIC with the LESC
- Wisconsin law enforcement cannot enforce civil immigration status violations - the NSEERS category. Therefore, the officer must release the person without delay but it is recommended by the Wisconsin Attorney General that law enforcement contact ICE or WSIC, after the person is released.
- Law enforcement may arrest or detain any subject regardless of their immigration status as reflected by NCIC, if they have suspicion or probable cause that the subject has violated Wisconsin law.

Flying Armed

Law enforcement officers who need to fly while armed should be aware of the requirements of the Transportation Security Administration (TSA) in these situations:

- All law enforcement officers flying armed must have received TSA approved training for officers flying armed. The training consists of a brief PowerPoint presentation.
- State/local law enforcement officers are also required to present a letter from their chief/ commanding officer on department letterhead, stating the officer's need to travel armed and including the officer's itinerary.

Officers will also be required to present an NLETS message from the TSA. This NLETS message will be sent upon request to the officer's employing agency, and will contain a unique alphanumeric identifier used for verification at the airport on the day of travel.

The NLETS message is being implemented to provide a more secure means of confirming the identity of law enforcement officers flying armed. Prior to flying, the officer's employing agency must send an administrative message to the TSA ORI of VAFAM0199. The message must contain the following information, in the specified order:

LEOFA	(indicates this is a law enforcement officer flying armed request message. Messages without this notation will be ignored.)
NAM/SMITH, JOE.	(full name of the flying officer)
AGY/ DANE CO SO.	(agency name)
BCN/BSO123456.	(the officer's badge or credential number)
OFC/STATE.	(type of officer, either state or local)
NAO/SMITH, GEORGE.	(name of authorizing official)
CRT/YES.	(has officer completed required TSA flying armed training?)
CPN/7031234989.	(cell phone number of officer, without dashes)
APN/2023456788.	(phone number of officer's agency, without dashes)
EIT/PRISONER.	(type of escorted individual, either prisoner or dignitary)
EIN/SMITH, JOHN.	(name of individual officer is escorting)
NOA/AMERICAN.	(name of airline)
FLN/AA1234.	(flight number)
DOF/122508.	(date of flight)
DAP/DCA.	(abbreviation of departing airport – for example, Milwaukee Mitchell=MKE)
CAP/EWR.	(abbreviation of connecting airport)
FDA/BOS.	(abbreviation of final destination airport

The Downside of Sharing Investigative Data

Reprinted with permission from the CJIS Link Volume 9, No. 2, an FBI publication

Could you be ignoring National Crime Information Center (NCIC) policy? Unfortunately, someone is. In at least five separate recent incidents, citizens have called the Terrorist Screening Center (TSC) with questions about detailed information they had read in terrorist records of the NCIC Violent Gang and Terrorist Organization File (VGTOF). How did unauthorized recipients gain access to the restricted information in the VGTOF? In legalese, the source was "unauthorized secondary dissemination." The problem can also be characterized as a breach of policy. Efforts by the TSC and the FBI CJIS Division to explain the policy to the NCIC user community have been only partially successful. So, what is the policy? And what's going wrong?

Policy statements are not necessarily memorable and compelling to their intended users. Here is the VGTOF overview policy statement pertaining to the dissemination of VGTOF information:

> VGTOF information is exclusively for the use of criminal justice agencies for criminal justice purposes. In no case should VGTOF information be disseminated to any noncriminal justice agency. The security measures to be accorded criminal history record information as set out in the NCIC Security Policy should be followed with respect to the VGTOF and the information contained therein.

Though the policy is a well-phrased, compact statement, what does it really mean? Some background information may be necessary for a clear understanding. To begin with, although the VGTOF information is unclassified, the NCIC user community should treat it as Law Enforcement Sensitive. This applies not only to the VGTOF terrorist record itself but also to the telephone number for the TSC that appears in the caveat preceding each terrorist record in the VGTOF.

The term Law Enforcement Sensitive pertains to information that must be shielded from unauthorized disclosure to protect many people, processes, and entities, such as sources and methods of collecting information, investigative activity, evidence, pre-trial investigative reports and their integrity. What happens if Law Enforcement Sensitive information goes astray? Unauthorized disclosure of that information might well influence the way government programs are carried out, affect how law enforcement activities unfold, and violate the privacy of individuals. Unauthorized disclosure is not merely a one-time, individual act. The consequences of its ripple effect are too numerous to count.

What's going wrong? The following scenario is an example of misusing investigative information contained in the terrorist aspect of the VGTOF: An officer makes a traffic stop, runs the license plate, and gets an NCIC VGTOF hit. In accordance with protocol, he calls the TSC and learns that the subject is potentially a VGTOF subject. Then, contrary to protocol, the officer tells the subject that he is on the VGTOF list.

What led to this officer's misuse of the VGTOF record? Was it just a mistake? Perhaps the officer didn't intend to divulge the VGTOF information, but somehow he did. All law enforcement officers know how to conduct interviews with suspects, but the VGTOF terrorist hit might have complicated the dynamic.

Here are a few reminders about the proper protocol related to a VGTOF (terrorist aspect) hit:

- All records contained in the terrorist portion of the VGTOF are labeled. It reads: "Possible Terrorist Organization Member - Caution." This is preceded by a caveat advising law enforcement that the individual may have possible ties or affiliations to terrorism. The instruction is to contact the TSC immediately.
- When a VGTOF terrorist record is returned in response to an NCIC inquiry, the individual about whom the inquiry was run should not be advised that he or she is on a terrorist watch list.
- A VGTOF terrorist record being returned in response to an NCIC inquiry does not mean that the individual encountered is identical to the individual for whom the VGTOF record was created. Law enforcement must contact the TSC to determine whether or not the individual who has been encountered is the known or suspected terrorist who is on the watch list. Personnel at TSC and the FBI's Counterterrorism Division will review classified, unclassified, and sensitive data sources in order to verify the subject's identity.
- If a terrorist record contained in the VGTOF is returned in response to an inquiry of NCIC, the individual receiving the response (that is, an employee of an authorized criminal justice entity) must follow the protocol set forth in the caveat that precedes the record. This protocol includes the instruction to contact the TSC by phone.

Many branches of the government are working hard to combat terrorism, but the success of these efforts hinges on the cooperation and participation of law enforcement personnel at all levels - local, state, and federal. If an agency receives a VGTOF terrorist response to an NCIC inquiry, there is only one right way to proceed: contact the TSC and follow instructions, being mindful that these instructions may differ on a case-by-case basis.

Another facet of the problem of unauthorized secondary dissemination of VGTOF data is the issue of unauthorized initial dissemination of the information. Not all agencies are authorized to receive VGTOF hits. In part, an agency's type of Originating Agency Identification (ORI) number indicates whether or not it may receive such information.

VGTOF data are investigative information. No comparison can be made between the data in criminal history records and the data in investigative files because there is a qualitative difference between them. By definition, the former reflects official action, such as an arrest. The latter does not necessarily involve previous official action. Because the information contained in the VGTOF is considered Law Enforcement Sensitive, only certain law enforcement agencies are authorized to receive it. The list below shows a few examples of who is and who is not authorized to receive information from the terrorist portion of the VGTOF in response to an NCIC inquiry. Although the agencies on the Not Authorized list may have an ORI number, they are not authorized recipients of VGTOF hits.

Examples of entities authorized to receive VGTOF data include Police Departments, Prison Officials, Customs and Border Protection Agents, Governmental Regional Dispatch Centers. Examples of entities NOT authorized to receive VGTOF data include Family Court, Department of Motor Vehicles, State Department of Education.

Bridging the gap between the policy requirements for proper use of VGTOF data and the implementation of the policy is a challenge. If the problem persists, it may warrant occasional NCIC sanctions. Alternatively, it may yield to renewed efforts to dispel misunderstandings within the NCIC user community.

Do You Know What This Is?


STATE OF WISCONSIN
Department of Justice
Division of Criminal Investigation

This identifies JOHN DOE as

ESSENTIAL BROADCAST PERSONNEL

Attorney General J.B. VanHollen

The bearer of this card has been granted authority to proceed to broadcast facilities in times of natural disaster to facilitate repairs or perform necessary maintenance on equipment used to communicate with the public. If a law enforcement official finds that conditions at the time of requested admittance risk the loss of life, serious injury or property damage, access may be denied.

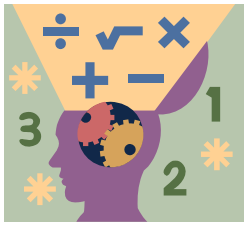
If there are any questions, contact the DCI Administrator at (608) 266-1671.

This is the Wisconsin Broadcaster Emergency Personnel ID Card. In cooperation with the Wisconsin Broadcasters Association (WBA), the Wisconsin Department of Justice – Division of Criminal Investigation has issued these cards to Broadcast Engineers statewide.

The purpose of this card is to identify Broadcast Engineers who are responsible for keeping radio and TV transmitters on the air. During a disaster, Sheriff Deputies and Police Officers may be presented with this card by Broadcast Engineers with the need to cross police lines to access their broadcast transmitters to keep emergency information flowing to the public. [Note: These cards are not for use by news-gathering crews.]

All Deputies and Officers in the field should be familiar with this card, and the importance of allowing these Broadcast Engineers through police lines if conditions warrant. Details on the program can be found on the WBA website at: www.wi-broadcasters.org/broadcasterid/

NCIC Math: DOE-DOW=?



Recent concerns at the national level regarding the timely entry of records into the National Crime Information Center (NCIC) database have resulted in a new report. Beginning December 1, 2008, each state will receive a report providing information comparing the Date of Warrant (DOW) and Date of Entry (DOE) fields for each wanted person record entered to NCIC. The first report will include information for the past three years. Subsequent reports will be for the prior six months and will occur on the first of June and December each year.

The report is broken down by Originating Agency Identifiers (ORIs), NCIC Number, Offense Code, Original Offense Code and the difference in time between the DOW and DOE. The difference between the DOW and DOE is broken down as follows:

Records entered the same day as the DOW (0)
Records entered up to 3 days later (1-3 days)
Records entered up to 10 days later (4-10)
Records entered up to 30 days later (11-30)
Records entered over 30 days later (>30)

The Crime Information Bureau will forward this report to the individual agencies. NCIC believes that making agencies aware of their own statistics in this area may assist in more timely entries of wanted person records in the future. To ensure maximum system effectiveness, NCIC policy states that records must be entered immediately when the conditions for entry are met, not to exceed three days upon receipt by the entering agency. This report compares Date of Warrant to Date of Entry only, and your agency may very well be in compliance.

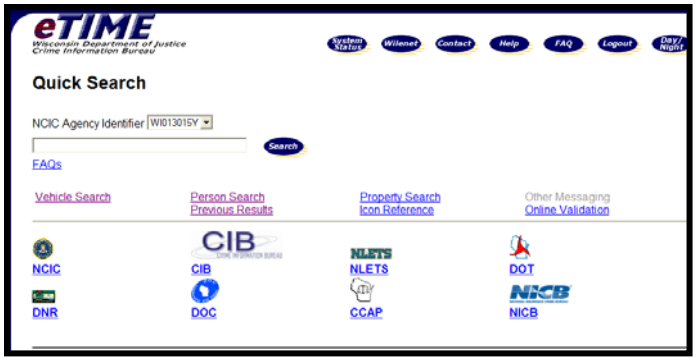
Disaster at Dispatch?

What would your agency do in the event of a disaster? 2008's record flooding and snowfall has many law enforcement/criminal justice agencies updating their disaster and evacuation plans. When making these plans, agencies should take the TIME System into account.

If personnel had to abandon your dispatch center or law enforcement building, what would happen to TIME System messages sent to your ORI? Agencies may wish to consider situations such as this, perhaps entering into an agreement with another agency to have messages sent to your ORI re-routed to them. In times of emergency, the TIMIE System Control Center can make such changes.

What about hit confirmation? The hit confirmation request may be received by another agency, but how would they respond? They could acknowledge receipt of the confirmation, explain the circumstances, and include a time frame in which a definitive answer is expected, but the agencies will need to work closely together so an accurate estimate can be provided. And what about longer term solutions? What if you were flooded out for days? Weeks? Longer? Could records be recovered? Could you even determine what records had been lost? Agencies may wish to expand their disaster planning to attempt to answer TIME System questions such as these.

Even More on *e*TIME



CIB is pleased to announce that effective December 14, 2008, several new queries are available to *e*TIME browser users.

*e*TIME browser users now have the ability to query NCIC property files, including stolen articles, securities (currency, bonds, etc.), vehicle/boat parts and stolen/lost/missing/recovered guns. Queries may be made by a serial number or owner applied number, or in the case of securities, queries may also be made by owner's name and/or social security number.

Users with *e*TIME certification only will be required to register for and successfully complete on-line training module 5, related to NCIC/CIB property files before having access to these transactions in the *e*TIME application. Users with a certification level higher than *e*TIME will automatically have access to these transactions if they are also an *e*TIME user. As with all TIME System training requirements, users with *e*TIME level access only are required to recertify every two years based upon the date of their last certification in order to keep their access active.

CIB website: www.doj.state.wi.us/dles/cib

TIME SYSTEM NEWSLETTER: The *TIME System Newsletter* is distributed to over 800 law enforcement, criminal justice and support agencies throughout Wisconsin. The purpose of the newsletter is to provide up-to-date information on the people, programs, events and technological advancements of the TIME System. The newsletter is published quarterly as a service of the Crime Information Bureau, Walt Neverman, Director. Writers mayl receive byline credits for submitted articles. Articles for publication and letters to the editor are welcomed. Log onto http://doj.state.wi.us/dles/cib for past issues of the *TIME System Newsletter*. Send all correspondence to Wisconsin Department of Justice, Crime Information Bureau, P.O. Box 2718, Madison, WI 53701-2718; Fax 608/267-1338; email cibtrain@doj.state.wi.us.

CRIME INFORMATION BUREAU
Walt Neverman, Director
17 W. Main Street
Mailing Address: P.O. Box 2718
Madison, Wisconsin 53701-2718
(608) 266-7314

Address Service Requested