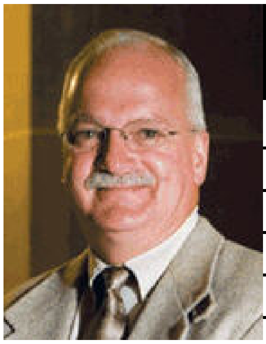
WISCONSIN DEPARTMENT OF JUSTICE
DIVISION OF LAW ENFORCEMENT SERVICES

J.B. VAN HOLLEN
ATTORNEY GENERAL

VOLUME 2011-2
FEBRUARY 2011

TIME System Newsletter
Crime Information Bureau

INSIDE THIS ISSUE:



As you read this newsletter DOJ and the Department of Transportation (DOT) will have either just implemented electronic sharing of Wisconsin driver license photos over the TIME System or be about to. The DOJ has set February 27th, 2011 as the go live date. This is a very exciting step forward for the TIME System and a long time coming.

Electronic sharing of the photo is just one requirement of the new state statute 165.8287. The statute also includes requirements to ensure proper use and confidentiality of the photo. I initially intended to replace my photo contained here with my DOT driver photo but realized this would be a violation of state statute. I recommend that agencies develop and implement policies and procedures to ensure your compliance with §165.8287 and §343.237. Additional information on this is contained in this newsletter.

So what's next? As you know CIB has been short staffed due to retirements and held positions open for budget reasons. The next priority is completing all of the TIME System audits for the 2009 – 2011 audit cycle. Audit schedules were adjusted in 2010 due to training officer / auditor vacancies most of the year. The TIME & Technical Unit is still one training officer short but is gearing up to complete the TIME System audits on schedule. If you have been expecting an audit, we have not forgotten you, and you will be hearing from us in 2011. Onsite audits for agencies that enter records will resume in mid February and mail audits of query only agencies have already begun. I appreciate your cooperation and assistance in completing our objective for 2011.

The May 2010 TIME Newsletter introduced you to NDEx (National Data Exchange). NDEx is a criminal justice information sharing system implemented by the FBI CJIS (Criminal Justice Information Services) Division. CJIS, the Wisconsin Department of Justice and the Wisconsin Office of Justice Assistance have worked together to contribute Wisconsin data to NDEx. The following agencies have signed an MOU and contribute data to NDEx today: Albany Pd, Barron Co So, Broadhead Pd, Glendale Pd, Green Co So, New Glarus Pd, Shorewood Pd and Whitefish Bay Pd. Milwaukee Pd is in the process of preparing their records for NDEx as well. NDEx provides tools for law enforcement to search, link, analyze and share criminal justice information such as incident/case report and arrest data, booking and incarceration data, and probation/parole data on a national basis. Query access is currently limited through CJIS' Law Enforcement Online (LEO) application. To obtain LEO access you must complete an application available at www.leo.gov. 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

WI Driver's License Photos—Proper Use

Wisconsin Act 167 created state statute 165.8287 and requires the Wisconsin Department of Transportation to make driver's license photos available to the Wisconsin Department of Justice in a digital format. Through the TIME System the Department of Justice must provide these photos to Wisconsin law enforcement agencies, federal law enforcement agencies, and law enforcement agencies of other states for the purposes of the administration of criminal justice and for traffic enforcement. Agencies are encouraged to review and develop internal policy and procedures to ensure proper use of Wisconsin driver photos as required by statute.

In accordance with this new statute, the TIME System will restrict access to the Wisconsin driver photo to only law enforcement agencies as defined by Wisconsin statute. District attorney's offices, Department of Corrections offices and facilities, social service agencies, etc. do not meet the statute's definition of a law enforcement agency, and thus the TIME System will block access to Wisconsin driver's license photos by these types of non-law enforcement agencies. Each Wisconsin driver's license photo returned via the TIME System will come with the following caveat as required by statute:

> THIS PHOTOGRAPH IS SUBJECT TO THE REQUIREMENTS AND RESTRICTIONS OF SECTION 165.827 OF THE WISCONSIN STATUTES. THE PHOTOGRAPH SHALL NOT BE USED FOR ANY PURPOSE OTHER THAN THE ADMINISTRATION OF CRIMINAL JUSTICE OR TRAFFIC ENFORCEMENT. SECONDARY DISSEMINATION IS PROHIBITED AND THE PHOTOGRAPH SHALL BE DESTROYED WHEN NO LONGER NECESSARY FOR THE PURPOSE REQUESTED. THE PHOTOGRAPH SHALL NOT BE USED AS PART OF A PHOTO LINEUP OR PHOTO ARRAY.

State statute 343.237 (8) requires that any agency receiving a Wisconsin driver photo keep it confidential and may disclose it only if disclosure is necessary to perform a law enforcement function, has attached to it the notation specified in (4m) and that the person to whom the photograph or fingerprint is disclosed agrees to destroy any copies of the photograph when it is no longer necessary to perform the law enforcement function for which the photograph was disclosed. As noted in the above caveat, any photograph obtained electronically by a law enforcement agency under this subsection may not be used for a photo lineup or photo array.

WI Driver's License Photos—Q & A

Several common questions have been asked related to Wisconsin driver photos:

Q Why do I have to include a purpose code if I query a WI DL photo?

A State statute requires that DOJ receive certification that the request for the photo was made for the purpose of either administration of criminal justice or traffic enforcement. Thus the only valid purpose code for a WI driver's license photo request is purpose code C.

Q Why do I have to include attention line/reason information when I query a WI DL photo?

A Statutes require the Department of Justice provide to the chief clerk of each house of the legislature an annual report concerning photographs released through the TIME System. The report must include information on to whom the photographs were provided and for what purpose the photographs were provided.

Q Will other states be able to access WI DL photos?

A Yes, the statute requires that DOJ provide Wisconsin driver photos to law enforcement agencies of other states. This will be accomplished through our interface with Nlets.

Q Can law enforcement agencies enter a WI DL photo in an NCIC person record?

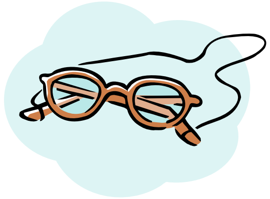
A No. The law requires certification that the request for a Wisconsin driver photo is made for a purpose of administration of criminal justice or traffic enforcement. Standard queries of NCIC do not require such a certification. In addition, the law requires a mandatory caveat to be returned with each Wisconsin DL photo. This required caveat cannot be appended to a NCIC record. There would be no way to comply with the state statute 343.237(4m) notation required for redisclosure of the photo.

Q Can law enforcement agencies authorized to receive a Wisconsin DL photo disseminate a copy to the District Attorney, Court or Department of Corrections?

A Yes if all conditions of state statute are met. Provisions of state statute 343.237 (5), (8), (9) and (10) shall apply to any photograph obtained electronically by a law enforcement agency under state statute 165.8287. State statute 343.237(8) requires that photographs and fingerprints be kept confidential and an agency "may disclose it only if the disclosure is necessary to perform a law enforcement function and the person to whom the copy of the photograph or fingerprint is disclosed agrees to comply with par. (c).

If a law enforcement agency discloses a copy of a photograph or fingerprint to another person under par. (a), the copy of the photograph or fingerprint shall have attached to it the notation specified in sub.(4m). Any person who receives a copy of the photograph or fingerprint from a law enforcement agency under par. (a) shall destroy any copies of the photograph or fingerprint in his or her possession when the photograph or fingerprint is no longer necessary to perform the law enforcement function for which the photograph or fingerprint was disclosed."

Transaction Specifications



Agencies with TIME System interfaces will need to work with their IT department or vendor if you want to request driver photos through your interface. The necessary changes will depend on the type of interface: 1)Legacy (text initiators) or 2) Server to Server (XML initiators).

Legacy interfaces will need to implement new transactions that are based on existing transactions plus three new fields: 1) DOT Image Indicator, 2) Purpose Code and 3) Attention / Reason. New transactions were required to provide the security and reporting required by state statute 165.8287. Server to Server interfaces will use existing schemas and elements to request the driver photo. To obtain transaction specifications contact Chris Kalina, TIME System Operations Coordinator at kalinaca@doj.state.wi.us.

CIB Technology Conference

For those of you who joined us at the 2010 CIB Technology Conference, thank you! Nearly 300 law enforcement and criminal justice personnel attended, enjoying numerous educational sessions on a wide range of topics. Attendees may want to check out the following website: http://www.doj.state.wi.us/dles/cib/conference.asp. Links on this website allow you to access copies of conference materials, submit your suggestions regarding the conference, and view a list of conference attendees. Planning is already underway for the 2011 CIB Technology Conference to be held Wednesday September 21, 2011 through Friday September 23, 2011 at the Radisson Hotel and Conference Center, Green Bay. We hope to see you there, so save the date!

~~Who is NOAH?~~ What is NOA?

If you are a user responsible for making entries to the TIME System, you need to know NOA.

The NOA, or Notify Originating Agency field, is a field that is available on all person and property entry screens. Some agency personnel assume they know what the NOA field means, and enter a 'Y' for yes every time they make an entry, thinking "Of course I want to be notified if someone finds my wanted person/stolen car/etc."

Unfortunately, that is not a correct understanding of the NOA field and its use. The NOA field should be used when the ORI believes that notification each time its record is hit on will provide investigative leads, *regardless of whether the location of the subject or property is known.* If "Y" is entered a flag will appear on the record, advising querying agencies to contact the ORI of the record. In addition, if the record is entered in NCIC, NCIC will send the agency a $H message each time their record appears in response to another agency's query. This may be the reason for some of the $H messages your agency may be receiving.

Agencies may wish to review the use of the NOA field with their entry personnel to ensure it is being used correctly and consistently by all personnel.

Did you Know…

That diploma certificates 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 chose 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.

TIME System Policies

The FBI's CJIS Security Policy establishes minimum information security requirements, guidelines, and agreements reflecting the will of law enforcement and criminal justice agencies for protecting the sources, transmission, storage, and generation of criminal justice information. The TIME System has adopted the CJIS Security Policy as the TIME System security policy. Did you know we have already written your department's TIME System Policies? Here at CIB, we have taken time out of our busy schedule to make your life easier. CIB has written a sample policy covering CJIS and TIME System requirements. Simply download the document off of the CIB website at http://www.doj.state.wi.us/dles/cibmanuals/ and modify it to your department's needs. It's as easy as that! Adopt the policy, and at future audits you will be prepared with required policies in place, as CIB staff have already done the work for you.

Have You Identified Your Unidentified?

Recent articles in a large Wisconsin newspaper have highlighted the growing number of unidentified bodies in the custody of local morgues/medical examiners. Has your agency identified all the possible unidentified human remains in your jurisdiction? A recent check of the NCIC Unidentified Person File found that Wisconsin agencies have a total of 24 unidentified persons listed in the file. The FBI and other organizations routinely report that the Unidentified Person File only contains entries for a fraction of the number of unidentified human remains actually recovered/in custody.

Agencies should check with their coroner or medical examiner to be certain that any unidentified remains are entered into the NCIC Unidentified Person File in hopes a match can be made with a missing person record and an identification made.

Social Security Information

The Social Security Death Index (SSDI) is a database of death records created from the United States Social Security Administration's Death Master File Extract. Most persons who have died since 1962 who had a social security number and whose death has been reported to the Social Security Administration are listed in the SSDI. For most years since 1973, the SSDI includes 93 percent to 96 percent of deaths of individuals aged 65 or older. It contains the records of over 84 million people. The SSDI is available free online from several websites. The SSDI can be a valuable tool for agencies when verifying wanted and/or other person records.

Ask CIB

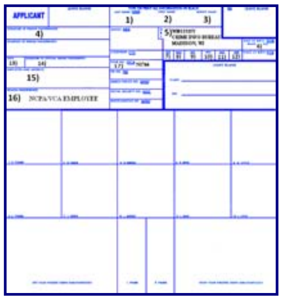
The 2010 CIB Technology Conference included the popular session 'Ask CIB', where attendees have the opportunity to ask CIB staff questions regarding TIME, TRAIN, eTIME, fingerprinting, or on any topic relating to CIB. Unfortunately, time constraints prevented all submitted questions from being answered. CIB has taken the submitted questions, compiled answers, and posted them on the conference website, http://www.doj.state.wi.us/dles/cib/conference.asp. Our hope is that this document will continue to grow as new questions are asked and answered, perhaps becoming a regular column or feature on the CIB or WILENET website.

New Portal 100 Features

The latest update to the Portal 100 software was made in early January 2011. Some of the features included in this update to the Portal 100 software are:

- New transactions to query a condensed WI driver's record.
- Update/refinement of urgent message function.
- New transaction to query WI driver summary record by name/additional identifiers.
- Updates to WI driver's query forms in anticipation of availability of WI DL photos (transaction is disabled at this time)
- Misc. code table updates.

Privacy Notification for Applicant Fingerprints


APPLICANT
1)
2)
3)
4)
5) WISCONSIN CRIME INFO BUREAU MADISON, WI
15)
16) NCPA/VCA EMPLOYEE

In order to comply with the requirements of the Privacy Act of 1974 and the E-Government Act of 2002, the FBI provides public notice of the categories of records it maintains in the Fingerprint Identification Records System. To provide continued compliance the FBI has implemented a procedure providing for the notification of potential fingerprint retention and subsequent uses of noncriminal justice fingerprint submissions. The FBI does not retain noncriminal justice fingerprint submissions for those individuals applying for license or employment governed by Public Law 92-544 (teachers, gaming, school bus drivers, security guards or other state licensed professions). The FBI retains noncriminal justice fingerprints submitted pursuant to federal law (Volunteers for Children Act, Adam Walsh Child Protection Act, Hazardous Materials drivers, etc.) only at the request of the submitting state. Wisconsin has not authorized the FBI to retain these fingerprints.

However a component of the Next Generation IAFIS will be a system called Rap Back. This option will allow entities submitting applicant fingerprints to the FBI to register for notification of future activity on the criminal history record of a previously submitted applicant. While this will eliminate the need for rechecks it also requires retention of applicant fingerprints to match against new arrest fingerprints being received.

It is the responsibility of the agency collecting or capturing the fingerprints and associated descriptive data to inform the person being fingerprinted of the authority to collect the information and its potential use. Therefore FBI has added a privacy notification statement to the back of the blue FBI applicant fingerprint card (form FD-258 revised 12-10-07) to alert applicants of the potential of fingerprint card retention and subsequent uses of noncriminal justice fingerprint submissions. Persons being fingerprinted on this form are required to provide a signature for verification and authorization at the time of fingerprinting. Any official capturing these fingerprints should advise the subject being fingerprinted to read the reverse side of the fingerprint card.

If an entity uses a livescan device to capture fingerprints for noncriminal justice purposes, the CJIS Division recommends that the agency should implement an electronic signature capability, provide a copy of the back of the FD-258 for the applicant to sign or provide a similar notice for the applicant to sign.

In order to assist entities in complying with this requirement CIB has requested a supply of the new FD-258 applicant fingerprint cards from the FBI bearing the privacy notice. Agencies submitting applicant fingerprints using blue FBI applicant fingerprint cards should request a supply of updated cards, destroying the old cards when the new forms are received. Criminal justice agencies seeking new applicant cards may contact Carol Brown at brownca@doj.state.wi.us or (608) 266-9585. Noncriminal justice agencies needing replacement applicant fingerprint cards should contact Kevin Sime at simeka@doj.state.wi.us or (608) 266-9398.

For those agencies capturing applicant fingerprints using a livescan device, CIB has developed a *Privacy Statement* form containing all the required notifications. This form is available online at www.doj.state.wi.us/dles/cib/forms. From the list of forms select *Privacy Statement*. These forms are to be retained by the entity requesting the fingerprint capture and are not to be sent to CIB.

In addition, persons being fingerprinted must be provided notice of their right to complete or challenge the accuracy of the information contained in either the FBI identification record or the Wisconsin Criminal History record. A second form has been developed advising applicants of their right to challenge the information returned. This form is also available at www.doj.state.wi.us/dles/cib/forms and is called *Challenge Notice*. For those entities using the Privacy Statement this information has been incorporated on the reverse of that form.

All entities capturing, submitting or receiving responses from fingerprint-based background checks should take the necessary steps to comply with these requirements as soon as possible.

Portal 100 and Windows 7 ®

Agencies using Windows 7 ® should note that the Portal 100 software is compatible with Windows 7 ® 32 bit operating system but is not and will not be compatible with Windows 7 ® 64 bit operating system. Use of the Portal 100 software with the Windows 7 ® 64 bit operating system is not supported by the vendor, CIB or TSCC.

Agencies using Windows 7 ® 64 bit operating system should be aware that any future updates to the Portal 100 software will not automatically be downloaded to terminals using the Windows 7 ® 64 bit operating system. The following options may work for agencies in this situation:

- Upon logging in after a Portal 100 software update is deployed, users at these agencies will receive an error message indicating the software is unable to find the update. Users can click on a link on this error page that will allow them to login to the previous version of the Portal 100 software. This error will appear on every login until the software is updated.
- When an update is available, agencies may uninstall the current version of the Portal 100 software and re-install the new software version.
- Agencies may contact their IT staff to make needed changes to run the Windows XP ® emulation mode on their Windows 7 ® 64 bit machine. The automatic update feature should then work correctly.

Nlets & License Plate Readers

Agencies are discovering license plate reader (LPR) data can be useful for investigative as well as patrol and parking enforcement purposes. Nlets now 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 now available to Nlets users. Nlets users can now 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. A new transaction, 0369, has been developed for the TIME System to allow users to query these databases and is located in the 'NLETS/NCIC Special Messages' section of the menu.

```
RR.ILNICBC00
12:18 11/18/2010 97141
12:18 11/18/2010 93604 WI0130000
*00216972XX
TXT
NICB RESPONSE FOR LIC/XXX111   MSG 001 OF 001
CROSSING LOCATION: INBOUND
ADDRESS: USCS-150 E JEFFERSON
CITY: DETROIT: TUNNEL          STATE: MI ZIP: 48226
CROSSING DT/TIME: 08/05/2010 00.37.18
LIC PLATE: XXX111     STATE: MI COUNTRY: U

** NOTICE **
THE NICB PROVIDES THE INFORMATION CONTAINED HEREIN SOLELY AS AN INVESTIGATORY
AID. SINCE THESE RECORDS ARE NOT VALIDATED, THE NICB DOES NOT GUARANTEE OR WAR-
RANT THEIR LEGITIMACY. PLEASE USE SECONDARY VERIFICATION BEFORE YOU TAKE ANY
ENFORCEMENT ACTION.
============================================================
RR.VANVS005V
12:18 11/18/2010 70247
12:18 11/18/2010 93609 WI013215Y
*00216972XX
TXT
Vehicle license plate number XXX111 was captured by mobile license plate recognition on August 23, 2010
near the intersection of Erin Dr AND Erin Ln, Eagan MN.

To access the complete LPR data record including other additional historical LPR scans, vehicle images and sat-
ellite map overlays, please proceed to the following Internet Website: http://nvls-lpr.com/nvls

Caveat: This is lead information ONLY to assist with your investigation and should NOT be used for non-law
enforcement purposes.  Should you require additional assistance with this RESPONSE, please contact National
Vehicle Service at 866-687-1102.
========================================================
```

*e*TIME Use

eTIME browser users should be aware of new *e*TIME use restrictions due to a change in the CJIS Security Policy. Using publicly accessible computers to access, process, store or transmit criminal justice information (as *e*TIME does) is prohibited. Examples of publicly accessible computers include (but are not limited to) hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.

Marquette University License Plates

The last TIME System newsletter announced the availability of Marquette University license plates. That article incorrectly listed the license plate type code used to query these plates via the TIME System. To query this plate via the TIME System, use license plate type code of **CV**. Stolen vehicle/license plate entries would use license plate type code CL (collegiate) for entry.

Fingerprint Background Checks — Who Needs Them?

CJIS & TIME System Policy require that fingerprint based state and national criminal history record checks be conducted within 30 days of initial employment or access for all personnel who will have physical or logical access to system terminals or unencrypted system data. Dispatch personnel who access the TIME System are included in this requirement, but don't forget about others who may have system access: records clerks, jailers, detectives that use the *e*TIME browser in their office, even officers operating mobile data computers in their squad cars. All are subject to this required fingerprint based background check.

What about your IT personnel/vendors? Those who have direct responsibility to configure and maintain computer systems and networks with direct access to FBI CJIS Systems are also subject to the fingerprint based background check requirement.

Don't forget about others who meet this requirement, such as cleaning personnel who have unescorted access to terminal areas or areas where TIME System data is kept. What about your department's clerical or administrative staff? Do they have access to terminal areas or areas where system data is kept? If so, they are also subject to the required fingerprint based background check.

The minimum check must include submission of completed applicant fingerprint cards to the FBI CJIS Division and the CIB through the state identification bureau. CIB and NCIC Wanted Person Files must also be checked. The good news is sworn personnel who have been fingerprinted and certified by the Wisconsin law enforcement standards board already meet this requirement. When fingerprint identification of the applicant/employee has been established and he/she appears to be a wanted person or to have an arrest history for a felony or serious misdemeanor, the employing agency *must* delay granting NCIC access until the matter is reviewed to determine if system access is appropriate.

License Plate Reader Leads

In conjunction with Nlets, the National Vehicle Service will begin to send stolen vehicle lead information over Nlets to law enforcement agencies across the country. Starting January 3, 2011 NVS will send an administrative message to notify law enforcement agencies of LPR reads that match active NCIC stolen vehicle records.

The following messages and format will be used:

STOLEN THEN READ (possible recovery location) (reported stolen then read) :

VIN 12345678901234567 as reported Stolen to NCIC by you on 02/12/20/2009, OCA 09-22411-B was Captured on a Digital Mobile Image on 02/06/2009 in Arizona, bearing License Plate Number KQY9685 near the intersection of Harlem and 183rd st. Phoenix , AZ

"This is lead information that the stolen Vehicle may be located in Arizona ." Please independently verify this information before you take any action.

DRY, NVS, VANVS006V, 1220 DST

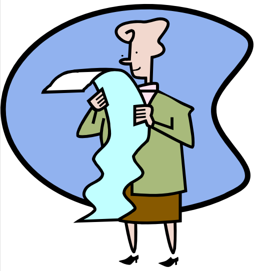
READ THEN REPORTED STOLEN (possible recovery fraud) (reported stolen after read date) :

VIN 12345678901234567 as reported Stolen to NCIC by you on 02/12/2009, OCA 09-22411-B in Arizona was Captured on a Digital Mobile Image on 02/06/2009 in Illinois bearing License Plate Number KQY9685 near the intersection of Harlem and 183rd st. Tinley Park, IL.

"This is lead information that the Vehicle may have been located in Illinois prior to it being Stolen, which could indicate possible fraudulent activity." Please independently verify this information before you take any action.

DRY, NVS, VANVS005V, 1200 DST

These messages indicate whether the vehicle's plate was read after the date of theft or prior to the date of theft for a state other than the reporting state.



Background Checks/Local Agency CHRI

Recently CIB was made aware of a law enforcement agency that requested criminal history record information from another agency using an administrative message. Agencies are reminded that requests for criminal history record information must be made using the proper specific CHRI request format. Requests for CHRI should not be made via administrative message. Agencies wishing to obtain criminal history record information from another local agency should use the proper transactions (0808/0809 for Wisconsin agencies, 0811/0812 for agencies in other states).

Portal 100 Software & IE 8

While the Portal 100 software is compatible with Internet Explorer 8, agencies that use Internet Explorer 8 (IE8) with the Portal 100 software should ensure the browser settings match those in IE7, and the enable automatic crash recovery setting (under tools/internet options/advanced) is unchecked. If these settings are not correct, any automatic updates to the Portal 100 software will not be correctly installed.

What is Validation?

Law enforcement has come to rely on the TIME and NCIC Systems as a reliable information gathering tool. Officers and others use the system to routinely query people and property, and may obtain information indicating a subject is wanted or missing or that property has been reported as stolen. But what happens when the information is incorrect or no longer valid?

What provides law enforcement with some level of confidence in records received from the TIME/ NCIC Systems? In order to answer that question, an understanding of where this information comes from is essential. Individual records in these files are entered and maintained by law enforcement agencies in Wisconsin and nationwide. Agencies contributing information to these files area obliged to regularly **validate** their records.

Validation obliges the ORI to confirm the record is complete, accurate, and still outstanding or active. Validation is accomplished by reviewing the original entry and current supporting documents. Recent consultation with any appropriate complainant, victim, prosecutor, court, motor vehicle registry files, or other appropriate source or individual also is required.

Agencies are reminded that validation *requires* the agency to make contact with the originator of the record (complainant, property owner, court, DA, etc.) to determine if the record entry is still valid. Is the missing person still missing, or have they returned home? Is the stolen car still stolen or was it just misplaced? Is the wanted person still wanted or has the warrant been dismissed/the fine paid? Failing to properly validate records can open an agency to possible civil or criminal liability.

To complete validation, an agency must place a check mark next to each record on your validation list, indicating that you have checked the record and taken proper action. Proper action may mean updating the record with new information, cancelling the record if is no longer needed, or no action at all may be needed. The check mark does not indicate the record is a valid, current record, but simply indicates that you have reviewed the record and taken any needed action.