Reviewed: 01/16/2026

WISCONSIN

TIME SYSTEM

2026 INSERVICE TRAINING

Table of Contents

Retention of Documentation

NCIC policy does not require agencies to retain documentation of entries that have been cleared from the TIME System. However, CIB recommends that the agency maintains documentation of the hit confirmation response and all relevant paperwork with the case file for a minimum of 18 months or the length of the case's life cycle. NCIC's guidance in the NCIC Operating Manual states: "The printout should be retained for as long as there remains any possibility that the defendant will challenge the arrest, search, or other law enforcement action taken because of the information contained on the printout. The printout should be retained until all possible levels of appeal are exhausted or the possibility of a civil suit is no longer anticipated."

As it pertains to keeping documentation for TIME system audits, CIB does not audit records that have been cleared by an agency. Once that record has been cleared from the TIME system, an agency is not required by CIB to keep the documentation. However, CIB does recommend maintaining the documentation from the case file for the same reasons mentioned above for a minimum of 18 months, or the case's life cycle. Agencies should refer to their own policies and procedures for document retention.

Vehicle Theft by Fraud and the Identity Theft File

Vehicles purchased by fraudulent means can be entered into the Stolen Vehicle file. The criteria for entering a stolen vehicle are as follows:

1. A stolen vehicle may be entered if a theft report has been made. The agency holding the theft report will enter the record.

2. The entering agency is responsible for keeping the record up to date.

3. Agencies must have documentation (either electronic or hard copy) on file to support the stolen vehicle entry.

4. All NCIC entries should be made only by the agency holding the theft report and having primary jurisdiction over the location of the actual theft (exception: dispatch centers on behalf of an agency).

Based on the above information, if a vehicle is purchased fraudulently in another state (i.e., California), then a stolen vehicle report must be made in California since that is where the vehicle was taken from. If the person whose identity was compromised / used resides in Wisconsin, that individual will need to file a fraud report with their local Wisconsin agency. CIB would then also strongly encourage the local agency to utilize the Identity Theft file to enter the victim's information into the TIME System. Documentation for the identity theft complaint must meet the following criteria for entry into the Identity Theft File:

1. Someone is using a means of identification of the victim (denoted in the Identity Theft and Assumption Deterrence Act of 1998 as any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual)

2. The identity is being used without the victim's permission.

3. The victim's identity is being used or intended to be used to commit unlawful activity.

4. There must be an official complaint (electronic or hard copy) recorded by and on file with the law enforcement agency.

5. The victim must sign a consent waiver prior to the information being entered into the Identity Theft File. This waiver is available on WILENET. (The waiver is not required for deceased individuals if law enforcement deems that the victim's information has been stolen).

6. If the identity of a thief is known and an arrest warrant has been issued, the agency should enter the victim information in the S/F fields in the Wanted Person File.

7. Only the agency that takes the identity theft complaint may make an NCIC identity theft entry (exception: dispatch centers on behalf of an agency).

Retention periods for stolen vehicles entered with a VIN or OAN are four years plus the year of entry. The retention period for the Identity Theft File is a maximum of five years. If either of those files reach the end of their retention period, the agency can re-enter the record if either the vehicle is still stolen, or the victim's identity is still being utilized.

NCIC One Crime Inquiry

This transaction allows the user to submit an inquiry for all information related to a crime based on ORI and agency case number (OCA), and optionally the date of entry (DTE). Users can direct an inquiry to one, multiple, or all file types. If no file type is specified, the system will search all files. Images are not returned through One Crime Inquiry. The NCIC One Crime Inquiry transaction is available via form 0942 in Portal XL.

This transaction is useful in instances when an NCIC hit response returns more than ten secondary hits. The following caveat will be included near the end of the response:

TO OBTAIN ADDITIONAL SECONDARY HITS, INQUIRE ON FBI, SOC, OR VIN FROM PRIMARY HITS. TO OBTAIN ADDITIONAL RELATED RECORDS, USE THE ONE CRIME INQUIRY (QI) TRANSACTION.

If a user receives this message, they should use One Crime Inquiry to obtain all the associated results. This message is commonly seen in instances where many items were stolen together such as guns or vehicles.

The following Database Name (DBN) fields can be searched.

A - ARTICLE FILE
B - BOAT AND VEHICLE/BOAT PART FILES
G - GUN FILE
M - MISSING PERSON FILE
P - LICENSE PLATE FILE
R - CANADIAN VEHICLE INDEX
S - SECURITIES FILE
U - UNIDENTIFIED PERSON FILE
V - VEHICLE AND VEHICLE/BOAT PART FILES

W - WANTED PERSON, GANG, IDENTITY THEFT, THREAT SCREENING CENTER, PROTECTION ORDER, NATIONAL SEX OFFENDER REGISTRY, PROTECTIVE INTEREST, IMMIGRATION VIOLATOR, SUPERVISED RELEASE, VIOLENT PERSON, AND FOREIGN FUGITIVE FILES

For any questions about using the NCIC One Crime Inquiry transaction, or if your agency wants specifications to integrate the transaction within your interface application, please reach out to cibtrain@wisdoj.gov.

Investigative Interest

The investigative interest supplemental record allows agencies to indicate that they have an investigative interest in an existing NCIC record. Until recently, Wisconsin agencies could only see when another agency had placed investigative interest on a record. The TIME system now has a transaction that allows Wisconsin agencies to add investigative interest to another agency's record.

Up to ten agencies (not including the record holder) may add an investigative interest supplement to the base record. The following NCIC files allow for an investigative interest supplement to be appended: Article, Boat, Foreign Fugitive, Gang, Gun, Identity Theft, Immigration Violator, License Plate, Missing Person, National Sex Offender Registry, Protection Order, Securities, Supervised Release, Unidentified Persons, Vehicle, Vehicle/Boat Part, Violent Person, and Wanted Person.

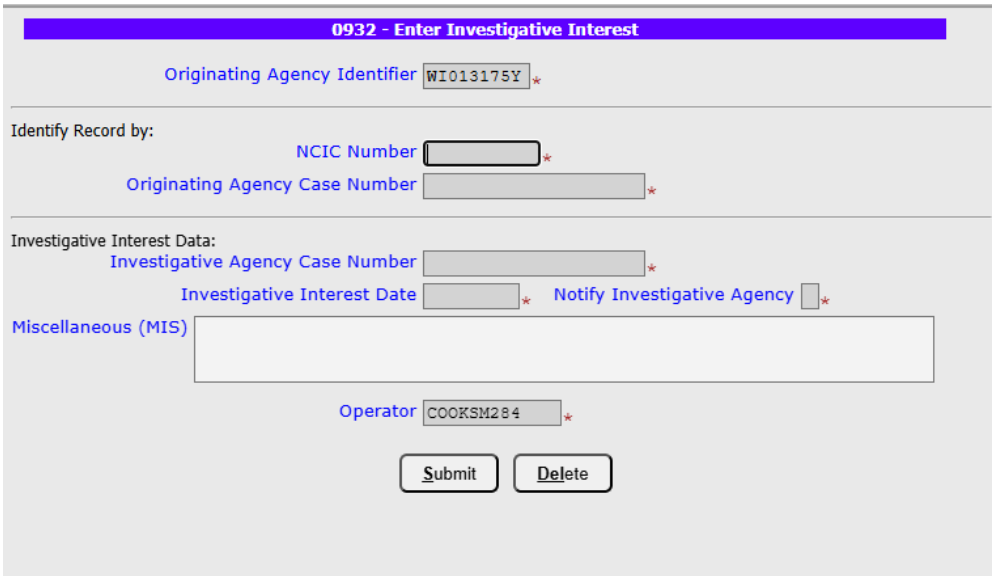
An example of when this might be used: Anytown PD enters a Wanted Person into NCIC. Bigberg PD has a homicide, and the suspect is the Wanted Person that Anytown PD entered. Bigberg PD does not have enough evidence for a warrant but wants to alert other agencies that they want to speak to the Wanted Person if located. Since the individual already has an entry in NCIC, Bigberg PD could add an investigative interest supplement to the existing Wanted Person entry so that if the individual is located/queried, other agencies would know that Bigberg PD needs to be contacted as well.

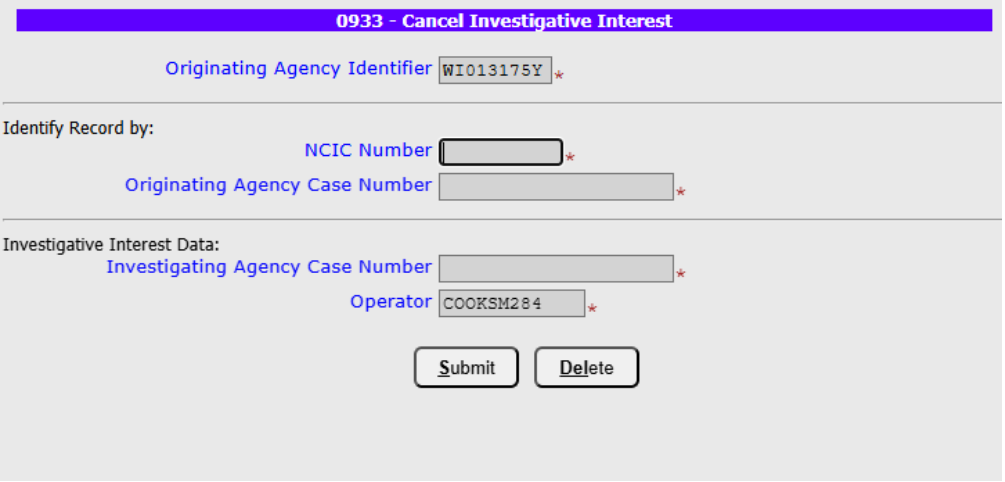
***MESSAGE KEY QW SEARCHES WANTED PERSON FILE FELONY RECORDS REGARDLESS OF EXTRADITION AND MISDEMEANOR RECORDS INDICATING POSSIBLE INTERSTATE EXTRADITION FROM THE INQUIRING AGENCY'S LOCATION. ALL OTHER NCIC PERSONS FILES ARE SEARCHED WITHOUT LIMITATIONS.
MKE/WANTED PERSON
EXL/1 - FULL EXTRADITION
ORI/MD1012600 NAM/SMITH, JOHN J SEX/M RAC/W POB/TX
DOB/19511012 HGT/510 WGT/175 EYE/BRO HAI/BRO
SKN/DRK SMT/SC R HND
FPC/121011CO141159TTCI13 MNU/AS-123456789 SOC/123456789
OLN/11111111 OLS/MD OLY/2000 OFF/HOMICIDE - WILLFUL KILL-POL OFF-GUN
DOW/19981201 OCA/92341244
WNO/635F1129 CTI/MD101261J
MIS/KNOWN TO COLLECT, DRIVE AND STEAL CLASSIC CARS
LIC/ABC123 LIC/MD LIY/2000 LIT/PC
VIN/2Y27H5LI00009 VYR/1975
VMA/PONT VMO/VEN VST/2D VCO/BLU
ORI IS ANY CITY PD MD 304 555-1212

DOB/19501012
NIC/W146203706 DTE/19991205 1400 EST DLU/20080616 1518 EDT
INVESTIGATIVE INTEREST AGENCIES:
IIA/WA1230000 ANY CITY PD WA 555 555-4321
ICA/123456789 DII/20010108
MIS/WANTED FOR QUESTIONING IN CONNECTION WITH MURDER INVESTIGATION
IMMED CONFIRM WARRANT AND EXTRADITION WITH ORI

Anytown PD will receive a $.I Entering Investigative Interest Notification when Bigberg PD enters the supplemental investigative interest record. Any other agencies that had also placed investigative interest in that record would receive a $.I notification.

Below are the Portal XL transactions to enter or cancel an Investigative Interest record. It is not possible to modify an Investigative Interest supplement; errors must be rectified by cancellation and re-entry.





Supplemental Investigative Interest records are kept for the same length of time as the base record. Once the base record's retention period ends, the agency that placed the investigative

interest will receive an "Investigative Interest Notification" confirming the record has been purged.

For any questions about how to use the Investigative Interest transaction or if your agency wants specifications to utilize the transaction within your interface application, please reach out to cibtrain@wisdoj.gov

Statewide Messages & Broadcasts

There are nine regions in Wisconsin to which agencies can send administrative messages. However, agencies are only permitted to send administrative messages to up to eight regions for a message. Agencies are not permitted to bypass the rules by sending the same messages to all nine of the regions via two separate administrative message transactions. For example, an agency might send a message to five regions in one message and then send the exact same message to the other four regions in a second message. This is a violation of TIME System policy: all requests for nationwide and statewide APBDs MUST first be directed to TSCC and they must be of significant importance to law enforcement. TSCC will evaluate and approve if the message falls within one of the following categories:

1. Death or aggravated battery to law enforcement officials involving a person at large (adequate physical description of the suspect and/or vehicle is required).

2. Felonies involving armed or believed to be armed fugitives (adequate physical description of the fugitive and/or vehicle is required).

3. Escapees from custody (includes escapees from officer custody, city and county jails, prisons, detention homes or centers, work camps and juvenile facilities).

4. Death and funeral notices of actively or formerly employed law enforcement officials. Wisconsin APBDs may also include public safety officials.

5. Attempts to locate (ATL) where foul play is suspected or known and is so specified (adequate physical description of the person and/or vehicle required). For death or serious illness message delivery (only if the direction of travel is unknown).

6. Found unidentified bodies or body parts (must be entered into NCIC prior to the broadcast request).

7. Severe weather warnings and disaster alerts.

8. Information that has statewide or nationwide law enforcement significance. Description of the method of operation requesting information on similar cases or alerting other agencies to be aware of the same.

Request for information on a person in custody refusing to cooperate by not giving name – (can request assistance based on description and circumstances of the case).

If the request concerns stolen property that cannot be entered into CIB/NCIC, the list of property items must have state or nationwide significance and must be condensed into 15 lines of text or less (Give general descriptions without listing all the quantities).

Any information that cannot be entered into CIB/NCIC and is pertinent to a criminal investigation that would be of interest to state or nationwide law enforcement agencies.

If the APBD request falls within one of the regulations and there is information in the APBD that qualifies for entry into any of the data files, the APBD will not be approved until the applicable data has been entered into CIB and/or NCIC.

9. Restrictions may be waived under the following conditions:

   a. A user has information that is pertinent to a criminal investigation that is of interest to ALL states and cannot be entered into NCIC.

   b. A user has information regarding kidnapping, skyjacking, or other serious criminal acts.

   c. A user has information on a wanted person that cannot be entered into NCIC but is of interest to ALL states.

One exception to getting approval from TSCC prior to sending out a statewide broadcast is using the mnemonic "ITLE" to send out an "Imminent Threat to Law Enforcement" message. Agencies do not have to direct a request to TSCC first. They can use the mnemonic ITLE, which will be sent out to all statewide law enforcement agencies only. At least one of the following criteria must exist to send 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.

3. Law enforcement officer missing in connection with official duties.

If your agency has any questions on what types of messages meet the statewide/APBD criteria, email cibtrain@wisdoj.gov.

NCIC Images

Images can be associated with NCIC records to assist in identifying a person or property. There are 3 different image types to choose from when entering a record. The following types of images can be stored for person records: mugshot, signature and identifying images. Identifying images can also be added to help identify property (articles, guns, boats, parts, vehicles, etc.)

Mugshot Image (IMT M): *A frontal face view from the shoulders to the top of the head is entered and maintained by an ORI and associated to a person.* Just because it is called a "mugshot" does not mean it has to be a booking photo. Use this image type for a frontal face view from the shoulders up of the wanted person, missing person, respondent, violent person, etc. This image type will appear if the querying agency turns on their NCIC image indicator.

Signature Image (IMT S): *An image of a signature is entered by an ORI and associated with a person.*

Identifying Image (IMT I): *An image which may help identify a person or property (scars, marks, and tattoos; photograph of a person; "aged" photograph of a missing juvenile, photograph of a*

vehicle or an article, etc.) is entered and maintained by an ORI and associated to a person, article, gun, part, vehicle or boat. If this type of image was entered, any agency that queries the record will not see the image unless they query the NCIC image number directly.

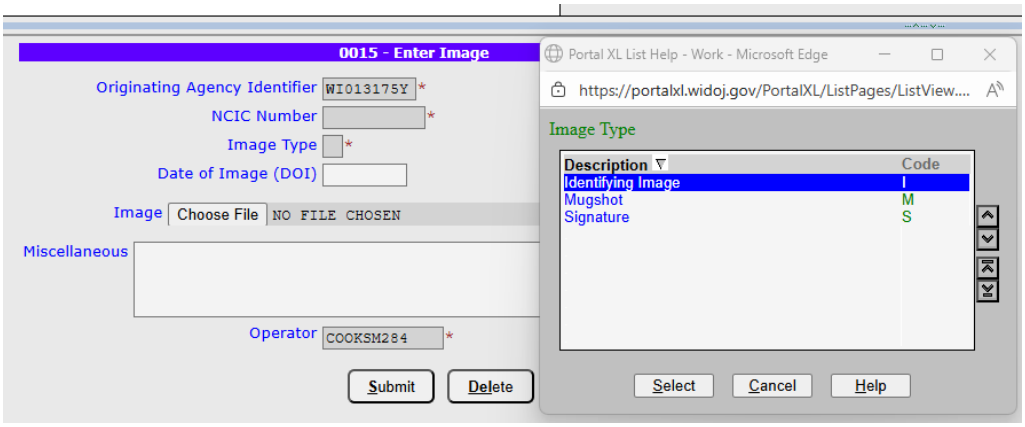
The rules for images are as follows:

- Only one "mugshot" can be associated with an NCIC person record.
- Only one signature can be associated with an NCIC person record.
- No more than 10 identifying images (other than mugshot and signature) can be associated with a person record.
- No more than 10 identifying images (tattoos, dress or graffiti) can be associated with a gang/terrorist group reference record.
- Only one identifying image can be associated with a vehicle/boat part, article or gun.
- Only one identifying or generic image can be associated with a vehicle or boat.
- Images must be in JPEG format with a size of 256 x 256 pixels and 8 bits per pixel in the workstation.
- WI Driver's license photos may **not** be entered as an NCIC image.
- Images are subject to the same validation requirements and retention periods as the records they are associated with.

When an image is entered/uploaded, the NCIC number (NIC) of the person or property must be included. The NIC links the image record with the person or property entry that already exists.

When a user queries a person or property, they may request that image information be returned *if available* by indicating 'Y' for yes in the NCIC image indicator field. For a person, this would be a mugshot; for property, it would be either the identifying image or the generic image. If a user wants to view all images associated with a record (identifying images for a person, etc.) they must use the query image transaction #0017 and query the NIC of the record in question.

An NCIC hit on an image record or hit response containing an image does not constitute probable cause to arrest. When an agency receives an image record(s) in response to an NCIC System inquiry, the hit must be confirmed with the ORI of each record. For example, if you queried an individual and their name came back with a wanted person hit and the photo attached to that record that looks exactly like the person you are out with, does not mean you can automatically arrest that individual. Complete the hit confirmation process with the entering agency prior to making the arrest.



Violent Person File

The Violent Person File (VPF) was designed with officer safety in mind; allowing a person search query to alert law enforcement officers that an individual they are encountering may have the propensity for violence against law enforcement. To enter an individual into the violent person file, they must meet one of the four NCIC entry criteria.

1. Offender has been convicted for assault or murder/homicide of a law enforcement officer, fleeing, resisting arrest, or any such statute which involves violence against law enforcement.
2. Offender has been convicted of a violent offense against a person to include homicide and attempted homicide.
3. Offender has been convicted of a violent offense against a person where a firearm or weapon was used.
4. A law enforcement agency, based on its official investigatory duties, reasonably believes that the individual has seriously expressed his or her intent to commit an act of unlawful violence against a member of the law enforcement or criminal justice community.

The VPF file type is underutilized. In Wisconsin, there are over a thousand individuals who meet one of the three conviction criteria, yet Wisconsin agencies have made fewer than 200 entries.

Perhaps an individual does not have warrants out for their arrest, and they are not on Probation; but they do have a Criminal History. If an officer on a traffic stop requests a name be run, that criminal history won't automatically come back unless a Criminal History of the individual is queried. The Violent Person entry will come back on a name query and alert the officer to the person's propensity for violence before getting to the point of querying a criminal history.

Any agency encountering an individual who meets one of the listed criteria is permitted to enter the individual into the Violent Person File. It does not have to be the agency in which the convicted offense occurred. If a user runs a criminal history and sees any of the convictions listed from the criteria or if they have documentation of the threat that the individual made, that agency may enter a violent person record.

CIB recommends that agencies establish policies and procedures to ensure proper use of the VPF file type. These policies can address internal concerns about who is authorized to enter records and whether social media posts can be used for documenting threats.

According to the NCIC operating manual, the VPF should be used if an individual meets one of the four criteria and documentation is available. Agencies can enter individuals who meet the criteria even if a policy is not yet in place, provided proper documentation is acquired.

Example: Madison PD has an initial encounter with an individual and they find an out of state conviction on criminal history that meets one of the 3 conviction criteria, Madison PD can enter the person into the VPF. They would include the documentation from the criminal history in the case file for the Violent Person File entry.

The Violent Person file (VPF) does not permit officers to detain or arrest an individual based solely on the return of the violent person record.

VIOLENT PERSON RECORD

WARNING-A SUBJECT IN THIS RESPONSE HAS BEEN IDENTIFIED AS A VIOLENT OFFENDER OR A SERIOUS THREAT TO LAW ENFORCEMENT OFFICERS. REVIEW THIS RESPONSE IN ITS ENTIRETY TO OBTAIN ADDITIONAL INFORMATION ON THIS SUBJECT. USE EXTREME CAUTION IN APPROACHING THIS INDIVIDUAL.

WARNING-THE SUBJECT IN THIS RECORD HAS BEEN IDENTIFIED AS A VIOLENT OFFENDER. THE SUBJECT HAS A CRIMINAL HISTORY OF ASSAULTING LAW ENFORCEMENT OFFICERS. USE CAUTION IN APPROACHING THIS INDIVIDUAL. DO NOT ARREST OR DETAIN BASED SOLELY UPON THIS INFORMATION.

Although some agencies may use an internal RMS to flag or track violent individuals, the use of this file type would allow for officers all over the country, who do not share an RMS, to be made aware of the safety issues involved with violent individuals. The retention period for this file type is indefinite.

TIME System Misuse

Information obtained from TIME/NCIC should only be used by law enforcement/criminal justice personnel and **only** for law enforcement/criminal justice purposes. If someone violates these (for example, an officer runs an individual for personal reasons) there may be internal, civil, and/or criminal penalties.

Each criminal justice agency authorized to receive NCIC/CIB information is required to have appropriate written standards for discipline of NCIC/CIB policy violators; however internal policy and discipline are not the only potential consequence. Depending on the circumstances and what type of information was improperly accessed, various federal and state laws may apply, including Title 28 CFR Chapter 1 Part 20 (access and use of III CHRI), Title 18 CFR Part 1 Chapter 123 (Federal Driver Privacy Protection Act), or various laws regarding computer misuse, misconduct in public office, bribery or privacy. Currently there

is no specific state statute dealing with TIME System use violations. If there is known misuse, it must also be reported to CIB.

Threat Screening Center File

Based upon Homeland Security Presidential Directive-6 signed in September 2003, the Threat Screening Center (TSC) was established to consolidate the Federal Government's approach to terrorism screening and to provide for the appropriate and lawful use of terrorist information in the overall screening process. The Attorney General has granted TSC the authorization to receive, store, maintain and disseminate identification records concerning other national security threat actors.

TSC is the only entity who has the authority to enter and update a record for an individual in the TSC file. They are required to keep either electronic or hard copy of documentation on file to support the record. The file type has an unlimited retention period. The record will remain on file indefinitely or until action is taken by TSC to modify or remove the record.

When an agency submits a NCIC wanted person query, the TSC file will be searched as well. If a positive TSC response is received, the receiving agency will receive a caveat that the individual cannot be arrested or detained solely based on that information. The inquiring agency will also be advised to contact TSC using a toll-free number, which is located in the response and the caveat.

There are 5 different handling codes utilized by TSC for their file records. The inquiring/receiving agency should adhere to the information and direction within the caveat.

***LEGAL NOTICE: UNAUTHORIZED DISCLOSURE IS PROHIBITED. THE INFORMATION IN THIS NOTICE BELONGS TO THE TSC AND IS PROVIDED TO YOUR AGENCY FOR OFFICER SAFETY, INTELLIGENCE, AND LEAD PURPOSES ONLY. USG ATTORNEY GENERAL AUTHORIZATION MUST BE OBTAINED PRIOR TO USING THIS INFORMATION, OR INFORMATION DERIVED THEREFROM, IN ANY LEGAL OR ADMINISTRATIVE PROCEEDING OR PROCESS. CONTACT THE TSC TO OBTAIN SUCH AUTHORIZATION. ***

When a positive TSC file response is received, the inquiring agency must **not** advise the individual that they may be on a United States Government (USG) watchlist. The unauthorized disclosure of USG watchlist information is **prohibited**. Information that an individual may be on a USG watchlist is the property of the TSC and is a federal record provided to the inquiring agency that may not be disclosed, disseminated, or used in any proceeding without the advance authorization of the TSC. This means that it is also prohibited to share / disseminate this information as part of discovery in a court case.