WISCONSIN

TIME SYSTEM

Training Materials

INSERVICE TRAINING

Revised 1/6/2016
(2016 Inservice Handout.doc)

CONTENT

CHRI Purpose Codes

The CIB training section has been fielding numerous questions from users relating to the proper use of purpose codes. 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. An explanation of each purpose code is included below.

CODE C CRIMINAL JUSTICE/LAW ENFORCEMENT PURPOSES

Acceptable by the Interstate Identification Index (III) and the state central repositories. Adult and juvenile records are accessible for this type of investigation.

Used for official duties in connection with administration of criminal justice. The term "administration of criminal justice" is defined as the performance of any of the following activities: detection, apprehension, detention, pretrial release, post-trail release, prosecution, adjudication, correctional supervision, rehabilitation of accused persons or criminal offenders. The administration of criminal justice includes criminal identification activities and the collection, processing, storage and dissemination of criminal justice information by governmental agencies. Social service cases involving child abuse, neglect or exploitation may be performed using a social service agency ORI ending in the letter "F".

Agencies may request a criminal history record check using purpose code C for the security of the criminal justice facility, for example:

1. 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. carpet cleaner, individuals responsible for maintaining vending machines, janitors, cooks, etc.
2. Volunteers at the criminal justice agency who are **NOT** involved with the actual administration of criminal justice at the criminal justice agency, e.g., participants in community ride along programs, volunteers at a confinement facility who are providing social or community services rather than rehabilitative services etc.
3. Confinement facility visitors.
4. Inmates of a confinement facility.
5. Inmate mail. A prisoner's list of names and addresses of those wishing to correspond with the prisoner. CHRI may be used when there is reason to believe that criminal activity is occurring or has occurred.
6. Participants of law enforcement-sponsored firearms training classes held at a public firing range or law enforcement facility.

CODE D CIVIL DOMESTIC VIOLENCE AND STALKING CASES

Acceptable by III and the state central repositories. CIB will return only adult records. III will only provide information that has not been sealed by the contributing state.

Civil and criminal court cases involving domestic violence or stalking cases (civil courts are issued a NCIC Agency Identifier with the letter D in the ninth position of the identifier). Law enforcement agencies providing CHRI to a criminal or civil court for a domestic violence hearing.

CODE F RETURN OF FIREARM(S) TO LAWFUL OWNER

Acceptable by the Interstate Identification Index (III) and the state central repositories. Adult and juvenile records are accessible for this type of investigation.

Used by criminal justice agencies for the purposes of issuing firearms-related permits and explosives permits pursuant to state law, regulation, or local ordinance; returning firearms to their lawful owners; and enforcing federal and state laws prohibiting certain persons with criminal records from possessing firearms in circumstances in which firearms have been pawned.

CODE H PUBLIC HOUSING APPLICANTS

Acceptable by III and the state central repositories. CIB will return only adult records. III will provide the identification segment of the record only. There is a cost for this type of request that will be billed to the ORI of the request. This code is prohibited when using the eTIME browser.

The Public Housing Authority (PHA) must submit a fingerprint card to the FBI to obtain the complete record. It is used to check the suitability of applicants for public housing under the authority of the Housing Opportunity Extension Act of 1996.

CODE J CRIMINAL JUSTICE EMPLOYEE APPLICANT CHECKS

Acceptable by III and the state central repositories. Adult and juvenile records are accessible for this type of background investigation.

This purpose code is used to initiate background checks of agency personnel. This includes:

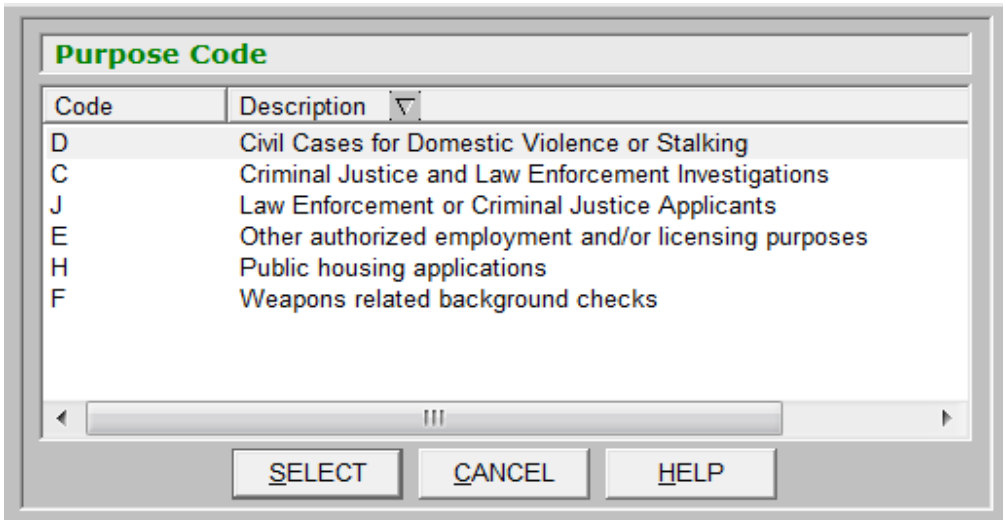
Noncriminal justice agencies that are involved with the administration of criminal justice on behalf of the criminal justice agency.

Vendors or contractors at the criminal justice agency who **ARE** involved with the actual administration of criminal justice at the criminal justice agency, e.g., personnel involved with maintenance of computer systems, upgrading records system, data entry clerk, etc.

Volunteers at the criminal justice agency who **ARE** involved with the actual administration of criminal justice at the criminal justice agency, e.g., volunteer dispatcher, volunteer data entry clerk, volunteers at a confinement facility who are providing inmate rehabilitation, etc.

CODE E AUTHORIZED EMPLOYMENT/LICENSING PURPOSES

Accepted by **some state central repositories only**, no other purpose code may be used to bypass this requirement and access III information for employment purposes. Only adult records are accessible for this type of background investigation. Authorized means that the criminal history inquiry is required by state statute, local ordinance or federal regulation. Agencies using the TIME System terminal to do this type of non-law enforcement background checks are encouraged to use http://wi-recordcheck.org instead. There is a cost for this type of request that will be billed to the ORI of the request. This code is prohibited when using the eTIME browser.



Extradition and Geographic Limitations

Communication must take place with the district attorney or prosecutor's office regarding extradition restrictions on felony and misdemeanor warrants entered into the TIME System. Documentation must be kept in the case file to support the extradition limitations entered. Your local law enforcement agency may develop their own geographic restrictions policy on how far they will go to serve civil process warrants. This policy must be in writing and available for review during an NCIC or CIB audit.

EXTRADITION

1. Before entering a record of a wanted person in NCIC, the entering agency must attempt to determine, to the maximum extent possible, if extradition will be authorized when the individual is located in another state. For NCIC purposes, extradition is the surrender by one state to another of an individual charged with or convicted of an offense outside its own territory and within the territorial jurisdiction of the other. Agencies entering warrants that do not meet the NCIC definition of extradition (e.g., intrastate only) must code the EXL Field as 4 (NO EXTRADITION – IN-STATE PICK UP ONLY. SEE MIS FIELD FOR LIMITS) for felony warrants or D (NO EXTRADITION – IN-STATE PICK UP ONLY. SEE MIS FIELD FOR LIMITS) for misdemeanor warrants. Additional details regarding intrastate limitations may be placed in the MIS Field.

2. In situations where an agency is absolutely certain that the wanted person will not be extradited, the individual's record may be entered in NCIC 2000 using the appropriate code in the Extradition Limitation Field. For NCIC Legacy-formatted messages, NOEX may be entered as the first four characters of the Miscellaneous (MIS) Field along with the additional details regarding the intrastate limitations.

3. At the time of entry, if there is a limitation concerning extradition of the wanted person, such information should be entered using the appropriate code in the Extradition Limitation Field with any specific limitations placed in the MIS Field of the record (NCIC 2000). For NCIC Legacy-formatted messages, the entering agency may place extradition limitation information in the MIS Field.

4. In many instances, however, no forecast of extradition can be made at the time the wanted person is entered on file because extradition is not a law enforcement decision. In such cases, use the codes 6 or F in the Extradition Limitation (EXL) Field to indicate PENDING EXTRADITION DETERMINATION. If at some future time, the entering agency learns that the individual definitely will not be extradited, the NCIC 2000 record must be modified using the appropriate code in the EXL Field. For NCIC Legacy formatted messages the entering agency must enter NOEX as the first four characters of the MIS Field.

5. When State Assigned Vehicle Identification Number (SVIN) is used with vehicular data included in the record, NOEX is placed second in the MIS Field. Additional information on SVIN can be found in the Vehicle File chapter.

EXTRADITION LIMITATION FIELD (EXL)

One of the following extradition limitation codes must be used when entering a warrant into NCIC. The extradition limitation field will be defaulted to a "1" (felony full extradition) for NCIC 2000 non-complaint software users.

1 = Felony full extradition
2 = Felony limited extradition see miscellaneous field
3 = Felony extradition surrounding states only
4 = Felony no extradition
5 = Felony extradition arrangement pending see miscellaneous field
6 = Felony pending extradition determination

A = Misdemeanor full extradition otherwise noted in the miscellaneous field
B = Misdemeanor limited extradition see miscellaneous field
C = Misdemeanor extradition surrounding states only
D = Misdemeanor no extradition
E = Misdemeanor extradition arrangements pending see miscellaneous field
F = Misdemeanor pending extradition determination

GEOGRAPHIC LIMITATIONS

Agencies and courts may geographically restrict wanted person entries, specifying what areas of Wisconsin the civil process warrant entry (ordinance or non-criminal state law) may be served. Agencies must have a written geographic restrictions policy on how far the agency will go to serve civil process warrants.

Standard geographical limitations have been defined for use in these circumstances. Agencies should not detain/apprehend persons if located outside the restriction area designated in the wanted person record.

An entry for a non-felony state law violation may list a geographic restriction, but only by court order (stated on the warrant or as an attachment to the warrant).

Total responsibility for geographically restricted warrants is that of the originating agency or the court.

IN-STATE GEOGRAPHIC RESTRICTIONS

Misdemeanor and felony warrants can only be entered with code A = Court Ordered - See Remarks. The specific restrictions must then be stated in the miscellaneous remarks field. Any of the geographic codes shown below may be used for entry of civil process warrants. Court ordered geographic restrictions must be stated on the warrant or as an attachment to the warrant by the judge.

A = Court Ordered – See Remarks
B = East of HWY 51
C = West of HWY 51
D = North of HWY 10
E = South of HWY 10
F = East of HWY 51 & North of HWY 10
G = East of HWY 51 & South of HWY 10
H = West of HWY 51 & North of HWY 10
I = West of HWY 51 & South of HWY 10
J = Within County of ORI
K = Within Adjacent Counties of ORI

Specific geographic restrictions reflected by one of the standard limitations must be explained in the Miscellaneous Remarks Field.

Locate

A Locate can only be placed AFTER Hit Confirmation has occurred.

The purpose of a locate message is to indicate (until the originating agency cancels the record) that the wanted person has been apprehended or stolen property has been located. If the ORI fails to cancel the NCIC record, the Locate will purge it within five days of placement. In the missing person file, a locate message indicates the whereabouts of the missing person has been determined and immediately purges the record from the file. If a CIB record is being located, TSCC will contact the ORI and explain why the locate is being placed against the record. TSCC will advise the ORI that they have approximately **TWO** hours to cancel the record. If the ORI fails to cancel the record within the time allotted, TSCC will cancel the record. This message is placed against a record that remains active in the system after hit confirmation has taken place. The locate message includes the date and time the person or property was located, as well as the name of the locating agency.

A locate message must be transmitted when an agency other than the originating agency of the record finds the missing person, apprehends the wanted person, or recovers the property on file in NCIC. It is recommended that a locate be placed against a CIB record after hit confirmation has taken place. **ALWAYS place a locate after going through hit confirmation on an NCIC hit.**

REASONS FOR PLACING A LOCATE

- Bond has been posted and the subject will be released but warrant is still entered. (NOEX)
- The ORI advises they will not extradite the subject, but the warrant has not been modified/canceled. (NOEX)
- The ORI advises they will extradite the subject, but the warrant has not been modified/canceled. (EXTR)
- The ORI advises to release the subject because the distance is too far or no personnel are available to transport, but the warrant has not been modified to reflect these geographic restrictions. (NOEX)
- The ORI advises to release the subject after giving him/her a new court date but the record remains in the system. (NOEX)
- Wanted person is being held on local charges / is incarcerated in prison. (DETN)
- Missing person is being detained and arrangements are being made for their return. (DETN)
- Missing person is not being detained and record has not been cancelled. (RELD)
- Property is recovered and is to be released with the record still in the system.
- Person or property is no longer wanted, missing or stolen and record has not been cancelled.
- Arresting/incarcerating agency refuses to place a locate and you want to add detainer data to the record.
- When ORI takes incorrect action.

****** Prior to placing a Locate against a wanted person record, make sure that your agency is within any geographical restrictions indicated on the warrant. ******

A Locate is placed against a record by contacting TSCC via administrative message (Portal 100 users may use form 1729). The message should advise:

1. The record to be located.
2. The reason for the Locate.
3. Your agency's case number assigned to this incident.

LOCATED RECORD ($.L.)

```
$.L.
WI018015G
LOCATE NOTIFICATION AT 1014 EST CCYYMMDD
LW.IN0450600.W123454321OCA/015664-A CCYYMMDD.
99-57B EXTR
LOCATING ORI IS GRIFFITH PD IN

MKE/ WANTED PERSON CAUTION
CMC/25-ESCAPE RISK
EXL/1-FULL EXTRADITION
ORI/WI018015G NAM/Test, Test E SEX/M RAC/W POB/WI DOB/19480105
HGT/602 WGT/250 EYE/HAZ HAI/BRO
SMT/SC LF ARM SOC/999999999 OFF/PROB VIOLATION-SEE MIS  DOW/19990815
OCA/015664-A
MIS/CHEM DEPENDENT ASSAULTIVE CONTACT PP AGENT 50204 AT 999 999 9999
IF NO ANSWER 608 267 9568 CONV ENDANG SAFE COND REG LIFE
SMT/MC DRUGAB   TAT UL ARM   TAT UR ARM
NIC/W111111111  DTE/CCYYMMDD 1231 EST DLU/CCYYMMDD 1231 EST
LOCATED/CCYYMMDD  IN0450600  99-57B EXTR
```

In one special circumstance NCIC allows for cancellation and re-entry of a Located Record:

- Hit confirmation has taken place.
- The ORI wants the subject and will transport the subject from the locating agency's state.
- The subject is released, awaiting extradition.

In this case the ORI may cancel and re-enter the warrant record. The ORI should state in the remarks field "Do not arrest in **(State of location);** subject awaiting extradition."

UNDERSTANDING THE LOCATE MESSAGE

```
 1 -   $.L.
 2 -   WI0______
 3 -   LOCATE NOTIFICATION AT 1014  EST CCYYMMDD
 4 -   L_.IN0______. NIC #OCA/______.
 5 -   99-57B EXTR
 6 -   LOCATING ORI IS ___________
 7 -   MKE/LOCATED (OR CANCELLED) ___________________
 8 -   ORI/____ NAM/________SEX/__RAC/__ POB/___ DOB/_______
 9 -   HGT/____ WGT/____ EYE/___ HAI/ ____
10 -   SMT/__________ SOC/__________ OFF/__________ DOW/________
11 -   OCA/ __________
12 -   MIS/ _____________________________________________________
13 -   MIS/ _____________________________________________________
14 -   SMT/MC DRUGAB  TAT UL ARM  TAT UR ARM
15 -   NIC/ ___________   DTE/ __________ 1231 EST
16 -   LOCATED/ ___________  IN0450600  99-57B EXTR
```

Line 1: Locate Message ($.L.) sent.

Line 2: The ORI of record being located.

Line 3: "Locate Notification" giving time (in Eastern Standard Time) and date of the Locate placement.

Line 4: Various data/descriptors. This line starts with a TWO CHARACTER CODE describing what is being located. The code will always start with the letter "L", followed by the first character of the FILE the located record is in (V/vehicle, W/warrant, M/missing, G/gun, etc.)

- The NCIC AGENCY IDENTIFIER of the locating agency will follow the two character locate/file code.
- Following the NCIC Agency Identifier will be TWO record identifiers. These may be NIC #, ORIGINATING AGENCY CASE #, SERIAL # The DATE the Locate was placed will follow. If there is a LOCATING AGENCY CASE #, it will follow the date the Locate was placed.

Line 5: The case number used in the locate request.

- If the record being located is a person, a code indicating what type of action is taking place will appear as the last data. The codes used are: EXTR (extradite), NOEX (no extradition) or DETN (Detained - used for Wanted and Missing Persons).

Line 6: LITERAL NAME of the AGENCY that is filing the Locate.

Lines 7-15: The record Locate is placed against.

Line 16: Shows the date the locate was placed, the ORI number of the agency that located the person or property and their case number used in the locate request.

Mental Health

A TIME System transaction has been created to allow law enforcement access to mental health records for the purpose of conducting background checks on individuals applying to become law enforcement officers. This transaction will only search the Mental Health records. Access to Mental Health records is available for all TIME System customers (eTIME, Portal 100, Server to Server).

> ***Act 223*** *provides a statutory mechanism for the DOJ to provide courts and law enforcement agencies access to orders not to possess a firearm resulting from certain mental health proceedings. Prior law did not allow courts to access mental health orders when considering the return of firearms to restraining order subjects at the termination of those restraining orders; nor did prior law allow law enforcement officers to access mental health orders when investigating possible violations of the possession of firearms.*

Transaction #0027 will allow the query through Portal 100:

Available through eTIME:

Access by Law Enforcement only for the purpose of conducting background checks on applicants for law enforcement officers.

Return of Firearms

Enacted in 2013, Wisconsin Act 223 authorizes access to mental health records by the courts and law enforcement for the return of firearms. The law also authorizes access to mental health records by law enforcement for determining the eligibility of law enforcement applicants for employment. Changes in federal law regarding National Instant Criminal Background Check System (NICS) authorize criminal justice agencies access to NICS information to conduct background checks for the purpose of returning firearms. To assist law enforcement when making a determination of whether an individual is restricted from possessing a firearm, a transaction was created in the TIME System to allow access to the mental health records and the National Instant Criminal Background Check System (NICS). This new functionality searches multiple data services including: CCH, CIB Hotfiles, DOC, DOT, III, NCIC, and NICS.

The NICS Background Check Law Enforcement guide is available for reference on the secure side of WILEnet https://wilenet.org/secure/html/resources/squadroom/NICS-LE-Guide.pdf.

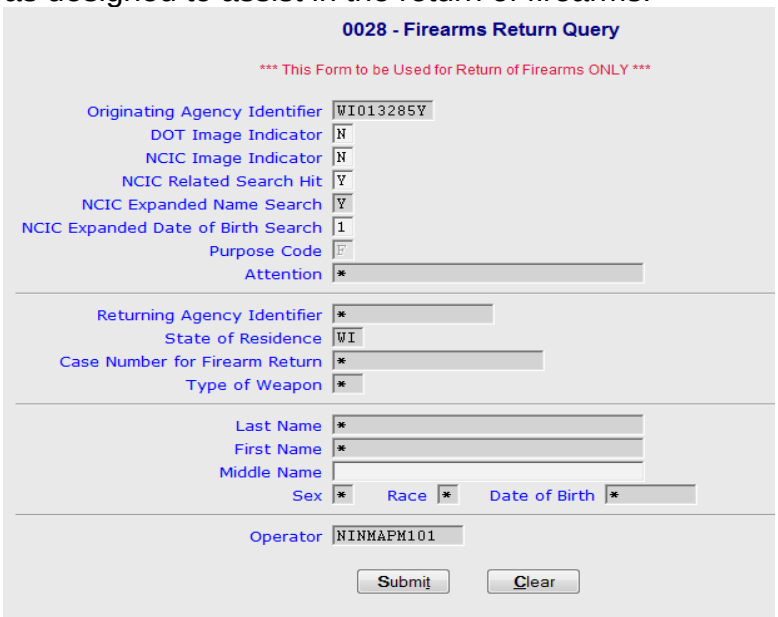
Proper CHRI purpose code for return of firearms is:

CODE F RETURN OF FIREARM(S) TO LAWFUL OWNER

Acceptable by the Interstate Identification Index (III) and the state central repositories. Adult and juvenile records are accessible for this type of investigation.

Used by criminal justice agencies for the purposes of issuing firearms-related permits and explosives permits pursuant to state law, regulation, or local ordinance; returning firearms to their lawful owners; and enforcing federal and state laws prohibiting certain persons with criminal records from possessing firearms in circumstances in which firearms have been pawned.

Portal Form #0028 was designed to assist in the return of firearms:



National Instant Criminal Background Check System (NICS)

Mandated by the Brady Handgun Violence Prevention Act of 1993 and administered by the FBI, the National Instant Criminal Background Check System, or NICS, is used by Federal Firearms Licensees (FFLs) to determine whether a prospective buyer is eligible to buy firearms. The NICS Index contains information provided by local, state, tribal and federal agencies of persons prohibited from receiving firearms under federal or state law. The NICS Index contains prohibiting information which may not be found in the NCIC or the III.

In 2014, changes were made to federal law allowing law enforcement agencies to access the NICS Index for purposes of conducting background checks prior to returning seized, stolen or abandoned firearms to lawful owners.

Law enforcement agencies accessing the NICS for the dispositions of firearms are able to search the prospective firearm transferees name and descriptive information against the records maintained in the III, the NCIC, and the NICS Index simultaneously. Agencies must have a valid ORI to access the NICS Index.

NICS Response:

NICS-INDEX-BEGIN
========== N I C S I N D E X ==========
RECORD FOUND BY:GENERATED AKA
NRI: 1599308140 STATUS: ACTIVE EXPIRATION DATE: N/A
PCA: B - Fugitive from Justice
NAM: LASTNAME, FIRST MIDDLE
SEX: U RAC: U HGT: N/A WGT: 0 EYE: XXX HAI: XXX
POB: N/A SOR: N/A
DOB: MM/DD/CCYY
SSN: N/A
AKA: N/A
SMT: N/A
MNU: N/A
MIS: STATE WARRANT IN MASSACHUSETTS - CONTACT (666)666-1234 WITH QUESTIONS
ORI: MACJIS085 OCA: 1241CR000735
DNY: N/A
DATA-SRC: MA
ARI: W8266052
CREATED DATE: 10/15/2012
UPDATED DATE: 10/15/2012
==========
MKE/SEXUAL OFFENDER

NAM/LASTNAME, FIRST MIDDLE

SEX/M RAC/W DOB/CCYYMMDD

HGT/600 WGT/220 EYE/BR0 HAI/BR0

CRR/SEX OFFENSE

CON/20000322
MIS/948-02(2) WI SEC0ND-DEGREE SEXUAL ASSAULT 0F A CHILD
OCA/00386722 ORI/WI013135C FBI/1234XXXXX

NIC/X272721212
NICS-INDEX-END

Protection Order & Injunction Files

No Contact Orders (conditions of bond ordering no contact), can be entered into the TIME System as well as Protection Orders and Injunctions. Here are guidelines to follow when entering, reviewing or validating these types of records.

TYPE OF ORDER

When entering No Contact Orders the proper type of Order would be Code #8, Other (entry of applicable statute number is required).

STATE STATUTE NUMBER

When utilizing type of order Other, Code "8", the State Statute Number found on the Protection Order/Injunction is required.

The statute field will be filled automatically in the response for record types "1" through "7" and "9" through "10". When the type of order is a type "11", "12" or "13", (Foreign Protection Orders), the state of issue, reason of protection order and restrictions should be included in the remarks field. Periods and parentheses are permitted in this field. Enter the statute number as it appears on the Protection Order/Injunction.

RESPONDENT

Enter the name as it appears on the face of the document.

Names with apostrophes (O'Neil, etc.) must be condensed by eliminating the apostrophe. For persons only using one name, enter that name as the last name and enter the letter "X" as the first name. For compound names enter both surnames with or without the hyphen. Each surname component must then be entered as a separate alias in a supplemental record. For oriental names the last name unit should be entered as the master last name. Each of the other units should then be entered as the surname in the alias field of a supplemental record, with the other units being used as the first and middle names. Each name combination must be queried separately. A wildcard (%) may be used in the last name field for DNR transactions only.

Enter only the first name or initial. If the person uses only one name, enter that name in the last name field and enter the letter "X" in this field. A wildcard (%) may be used in the first name field for DNR transactions only.

PETITIONERS

When the petitioner on the order is a business, the information should be entered as it appears on the court order. If there is no individual named on the order, enter the business name as it appears on the order into the last name field and place an X in the first name field.

When multiple petitioners exist, the first petitioner's information should be entered in the petitioner fields. Additional petitioners and their information should then be added in the supplemental petitioner fields.

Juveniles may appear as petitioners on an order. Their information should be entered in the petitioner fields, regardless of age. Listing juveniles in the remarks field is inadequate, as the remarks field is not a searchable field.

When entering No Contact Orders the proper type of Order would be Code #8, Other (entry of applicable statute number is required). Entry of these orders is not mandatory but recommended to protect the victim and can be performed by either a Sheriff/Police Department. Expiration date will be the respondents next court date and Petitioner data can be obtained from the court.

NOTE: NCIC requires the petitioner's name and either the date of birth or social security number for entry. If the petitioner information is entered without one of these fields the petitioner's name will not appear in the NCIC record. The name will still appear in the CIB record. However, a query of that name will not produce the record.

EXPIRATION DATE

Expiration date for No Contact Orders will be the next court date as deemed by the Courts.

Contact and ongoing communications will be necessary between the entering agency and Clerk of Courts to maintain the correct expiration date as the No Contact remains in force.

Protection Order Response:

```
/0022 1742 9D734BAF                  WI013285Y
CIB    160756      2 11/23/15 09:20 01 OF 01
***** PROTECTION ORDER/INJUNCTION - OTHER *****
** SEE THE MISCELLANEOUS FIELD FOR COMMENTS REGARDING THE TERMS AND CONDITIONS OF THE ORDER

SERVICE SERVED

COURT
   COURT CASE #/2015TEST  COURT ORI #/WI013023J
   BEGINNING DATE/11232015  ENDING DATE/01042016
   STATUTE #/947.01
RESPONDENT
   NAME/TEST, JAMES
   SEX/MALE  RACE/WHITE  DATE OF BIRTH/11231998
   HEIGHT/511  WEIGHT/185  HAIR COLOR/BROWN
DETAIL
   ORI/WI013285Y  ORI IS CRIME INFORMATION BUREAU
   SYSTEM IDENT #/11111111  NCIC #/H111111111
   AGENCY CASE #/2015TEST
   ENTERED BY/NINMAPM101  DATE/11232015  TIME/0920
PETITIONER
   NAME/NA, NA
REMARKS
   SHALL APPEAR ON ALL COURT DATES SHALL GIVE WRITTEN NOTICE TO COC WITHIN 48 HRS OF ANY CHANGE
   OF ADDRESS OR TELEPHONE NUMBER SHALL NOT COMMIT ANY CRIME SHALL NEITHER DIRECTLY NOR
   INDIRECTLY THREATEN HARASS INTIMIDATE OR OTHERWISE INTEREFERE WITH VICTIMS OR WITNESS IN THIS
   ACTION FOR NAMES OF VICTIMS PLEASE CONTACT BDPD AT 0000000000  SUBJECT CURRENTLY OUT ON
   SIGNATURE BOND

*****VERIFY STATUS IMMEDIATELY WITH ORI*****
```

CCAP

The Consolidated Court Automation Programs (CCAP) provides access to certain public records of the circuit courts of Wisconsin. The information displayed is an exact copy of the case information entered into the CCAP case management system by court staff in the counties where the case files are located. The information provides the type of case, the parties, and any judgment that has been entered in the case. For criminal cases, a case summary is provided to show the current pending charges or the defendant's conviction/acquittal status. Criminal cases, traffic, and ordinance violations also show a history of the charges against the defendant. A link to "court record events" provides the date of actions taken in the case, such as filing of the complaint or petition, pleadings, court appearances, and judgments. Individual courts vary in how much detail is entered for each court record event.

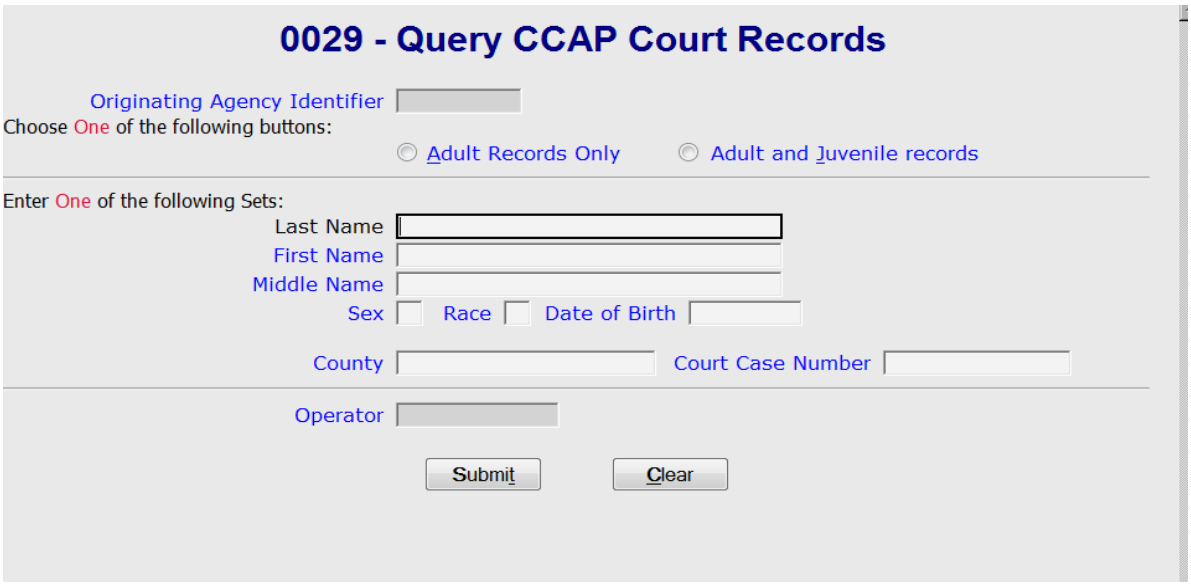
ACT 270 allows the following:

938.396 (2g) (c) law enforcement agencies. Upon request of a law enforcement agency to review court records for the purpose of investigating alleged criminal activity or activity that may result in a court exercising jurisdiction under s. 938.12 or 938.13 (12), the court assigned to exercise jurisdiction under this chapter and ch. 48 shall open for inspection by authorized representatives of the requester the records of the court relating to any juvenile who has been the subject of a proceeding under this chapter.

Act 270 requires the state court to make juvenile data available to:

- Court Officials
- Prosecutors
- Law Enforcement Agencies for purposes of investigating alleged criminal activity which may result in a juvenile court exercising jurisdiction

PS Portal Form #0029:



eTIME Access:

System Security

The TIME/NCIC Systems are criminal justice computer networks that provide access to sensitive and sometimes confidential information, such as driver's license records, criminal history records, wanted person records, etc. This information must be protected from those who would try to gain unauthorized access to the system and those who would use information obtained from the system for unauthorized purposes.

Various agencies have agreed to make their information available to law enforcement and criminal justice via the TIME and NCIC Systems for the specific purpose of facilitating the administration of criminal justice. Any misuse of this information or violation of the understandings and policies of the system jeopardizes the availability of information for all participating agencies.

The FBI's CJIS Security Policy establishes *minimum* information security requirements to protect information sources, transmission, storage, and creation of criminal justice information. The TIME System has adopted the CJIS Security Policy as the TIME System Security Policy. Each agency and user accessing the system is responsible for ensuring the security of the system and criminal justice information.

AUTHORIZED PERSONNEL

TIME/NCIC System information is only to be used by *authorized* law enforcement/criminal justice personnel for law enforcement/criminal justice purposes. Authorized personnel are those that have undergone the required fingerprint based background check, completed security awareness training and appear on the agency's list of authorized personnel.

SYSTEM USAGE

TIME/NCIC System information is ***only*** to be used by authorized law enforcement/criminal justice personnel for law enforcement/criminal justice purposes. Both conditions must be met, for example, a law enforcement officer may not obtain license plate/vehicle registration information for personal reasons.

Each criminal justice agency authorized to access the TIME/NCIC Systems is required to have a written policy for discipline of policy violators. Misuse of the TIME System or information obtained from it may be a violation of state or federal laws, and violations may subject individuals and agencies to criminal prosecution and/or other penalties. The unauthorized request, receipt, or release of TIME/NCIC System information can and *has* resulted in criminal/civil proceedings.

PHYSICAL ACCESS & VISITORS

Agencies must control all entrances to the secure area and must verify that an individual qualifies for access before granting admission. Remember, authorized personnel are those that have undergone the required fingerprint based background check, completed security awareness training and appear on the agency's list of authorized personnel. If a person has not met these requirements, they may only access the secure area if they are escorted by someone who is authorized.

Before granting such a visitor escorted access to the secure location you should verify the visitor's identity. Visitors must be escorted at all times and visitor activity must be monitored.

Personnel should be aware of their surroundings and take steps to ensure unauthorized persons do not access criminal justice information or the TIME/NCIC Systems. This may include challenging or questioning unescorted subjects, verifying credentials of strangers, and/or ensuring visitors and other unauthorized users are not looking over someone's shoulder to get information. Numerous techniques and tools exist to help ensure the security of data. These may include the use of screensavers, screen shields, terminal location and positioning, etc.

Agency personnel should ensure that all people abide by entrance and exit procedures, visitor control, handling procedures, and access control points. Personnel should report violations or suspected violations, including areas that may not be secure.

Using publicly accessible computers to access, process, store or transmit criminal justice information is prohibited. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.

LOGINS

A unique login id is required for each individual who is authorized to store, process, and/or transmit criminal justice information. This includes all persons who administer and maintain the system/network that accesses and/or transmits TIME/NCIC information. Users are required to uniquely identify themselves before they are allowed to perform any actions on the system.

By logging in to and accessing the system and the information contained therein, users are signifying their agreement to abide by all system policies and procedures and acknowledging the possible consequences of misuse of system resources or criminal justice information. *Users should protect their logins and not share them with anyone.* Users are responsible for any and all system activity that happens under their login.

If a user is unable to login after 5 consecutive invalid access attempts, their account will be automatically locked for at least 10 minutes unless released by an administrator. In addition, the system will initiate a session lock after a maximum of 30 minutes of inactivity. The session lock will remain in effect until the user once again establishes access using appropriate login and authentication. In the interest of officer safety, devices that are part of a criminal justice conveyance, used to perform dispatch functions or designated solely for the purpose of receiving alert notifications and are staffed when in operation and located within a physically secure location are exempt from this requirement.

PASSWORDS

Passwords used to access the TIME/NCIC Systems must meet criteria to be secure passwords. Passwords must be at least 8 characters, must not be a dictionary word or proper name, and cannot be the same as the userid. Passwords must expire at least every 90 calendar days and cannot be identical to the previous ten passwords used. Passwords cannot be displayed on screen when entered, and must not be transmitted in the clear outside the secure location. *Users should protect their passwords and not share them with anyone.*

System users should be aware of subjects attempting to obtain computer system access or password/login information by using 'social engineering'. Social engineering means manipulating people into doing something or divulging confidential information. This may include emails from unknown sources, email attachments containing spyware programs, telephone callers purporting to be from another authorized agency, etc. When in doubt, system users should verify the source or identity behind the email, telephone call, etc. before potentially misusing system resources or providing criminal justice information to unauthorized subjects.

PROPER HANDLING OF CRIMINAL JUSTICE INFORMATION

Information obtained via the TIME/NCIC systems, whether in paper form or saved digitally, must be stored in a secure area inaccessible to the public.

Criminal justice information obtained from the TIME/NCIC Systems should remain in the secure area unless there is specific authorization and procedures for taking the information out of the secure area. When TIME/NCIC information (paper or digital) is transported outside of the secure areas it must continue to be protected, thus transport of TIME/NCIC information is restricted to authorized personnel.

TIME/NCIC information must be securely disposed of when no longer needed. Destruction of paper information may be accomplished by shredding, incineration, etc. Digital media storing TIME/NCIC information (hard drives, flash drives, CD's, etc.) must be sanitized or degaussed using approved sanitizing software that ensures a minimal 3-pass wipe. Inoperable digital media should be destroyed (cut up, smashed, shredded, etc.). The disposal or destruction of TIME/NCIC information must be witnessed or carried out by authorized personnel to avoid the possibility of inadvertent release of system information to unauthorized persons.

DISSEMINATION OF CRIMINAL JUSTICE INFORMATION

Any individual authorized to use the TIME/NCIC System who receives a request for system information from another individual must ensure the person requesting the information is authorized to receive the data. The correct Originating Agency Identifier (ORI) must be used in each transaction to identify the agency receiving the information to ensure the proper level of access for each transaction.

Each data service has its own rules for secondary dissemination of records, which may include requirements for logging, identification of the purpose of the request, and identification of the specific individual receiving the record. Most records may be legitimately disseminated to another criminal justice employee/agency when the purpose of the request is criminal justice related.

Any secondary dissemination of this information must meet state and federal statutes and/or regulations.

Criminal justice information obtained from the TIME/NCIC Systems may not be included in an internet email transmission unless the email is encrypted to the FIPS 140-2 standard. When email contains sensitive information, it should be standard practice to label those items as well.

Voice transmission of criminal justice information (via police radio, cellular phone, etc.) is exempt from the encryption and authentication requirements when an officer determines there is an immediate need for the information in a situation affecting the safety of the officer or the general public, or the information is needed immediately to further an investigation.

SECURITY INCIDENTS & RESPONSE

A security incident is a violation or possible violation of policy that threatens the confidentiality, integrity or availability of TIME/NCIC information. There has been an increase in the number of accidental or malicious computer attacks against both government and private agencies, regardless of whether the systems are high or low profile.

Indicators of a security incident may include system crashes without a clear reason, new files with novel or strange names appearing, changes in file lengths or modification dates, unexplained poor system performance, etc.

Personnel should know how to report a security incident, who to report an incident to, when to contact that person, and what basic actions to take in case of a suspected compromise of the system. This may include contacting a supervisor, contacting on-call information technology staff, disconnecting the affected computer from the network, etc.

Agency staff should document any security incidents/possible security incidents, and promptly report incident information to the Crime Information Bureau. Evidence of the security incident may need to be collected and retained to conform to the rules of evidence in case of legal action (either civil or criminal).

Agencies must monitor physical access to the information system to detect and respond to physical security incidents, and use automated mechanisms to make security alert and advisory information available throughout the agency as appropriate.

VIRUS/SPAM/SPYWARE & MALICIOUS CODE PROTECTION

To ensure information security, agencies connecting to the TIME/NCIC Systems are required to have in place malicious code protection, virus protection, spam protection and spyware protection. Users should be cautious when downloading internet content or clicking on web-based pop-ups/windows, unknown emails, email attachments or embedded objects. Removable devices such as flash drives, CDs, etc. may also possibly introduce viruses/malware and caution should be used before they are introduced to the system. Follow your agency's policies regarding use of such items.

Technical Considerations

MOBILE DEVICES – HANDHELD DEVICES, LAPTOPS, etc.

As digital handheld devices continue to become more integrated into the mobile workforce, security measures must be employed since such devices may be used outside of physically secure locations. Wireless devices, even in physically secure areas, are susceptible to penetration, eavesdropping and malware. Furthermore, compromised or lost wireless devices may introduce risk to the overall security of an agency's network, criminal justice information and/or the TIME/NCIC Systems. The use of digital handheld devices and/or laptops to access TIME/NCIC information is allowed, provided the agency implements the security requirements for such access as outlined in the CJIS Security Policy. This may include advanced authentication, encryption, security-related updates, official use guidance, data at rest encryption, and prevention of data compromise in case of possible loss of the device. The requirement to use or not use advanced authentication is dependent upon the physical, personnel and technical security controls associated with the user location as specified in the CJIS Security Policy.

Personally owned information systems shall not be authorized to access, process, store or transmit criminal justice information unless the employing agency has established and documented policies and procedures for such use. All devices must be authorized and must meet the requirements set forth by the CJIS Security Policy.

A personal firewall must be employed on all devices that are mobile by design (i.e. laptops, handhelds, personal digital assistants, etc.).

Mobile devices used to access the TIME/NCIC Systems may be agency owned or personally owned. Personally owned equipment used to access the TIME/NCIC Systems or used to access data obtained from those systems must meet all the requirements set forth in the CJIS Security Policy. Agencies wishing to use personally owned devices for system access must first document the specific terms and conditions for such use. Such documentation should consider licensing issues, agency control, security requirements, and sanitization of the device if the owner no longer carries out law enforcement duties, etc.

ACCOUNT MANAGEMENT

User logins/accounts should be kept current, when a user is terminated, leaves employment or job duties no longer require TIME/NCIC System access the user's system account should be disabled. An agency must validate system accounts at least annually.

User TIME/NCIC accounts will be assigned according to the principle of 'least privilege'. Least privilege means giving a user account only those privileges which are essential to perform assigned duties. Assigned authorizations will control access to the system and system information.

Users may only have one active computer session accessing the TIME/NCIC Systems at a time. Multiple concurrent active sessions for one user are prohibited unless the agency can document a business need for such multiple session access.

SYSTEM UPDATES

Malicious code protection, virus protection, spam protection and spyware protection must be in place at critical points throughout the networks and on all workstations, servers, and mobile computing devices on the network. Malicious code protection must be enabled, and must include automatic updates for all systems with Internet access. Agencies with systems not connected to the Internet must implement local procedures to ensure malicious code protection is kept current (i.e. most recent definitions update available). Resident scanning must be employed.

Agencies must monitor applications, services, and information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws. System patches shall be installed in a timely manner.

BACKUP & STORAGE PROCEDURES

Agencies must consider the requirements for secure storage of digital media and hardware containing criminal justice information, and ensure that such backup procedures, archiving, and storage, whether centralized or de-centralized (off site) meet the security requirements outlined in the CJIS Security Policy.

CIB Contacts

	Name	Telephone	Fax Number	Email
Director	Walt Neverman	608-264-6207	608-267-1338	nevermanwm@doj.state.wi.us
Deputy Director	Dennis Fortunato	608-267-2235	608-267-1338	fortunatodj@doj.state.wi.us
TIME & Technical Services Manager	Courtney Doberstein	608-266-0872	608-267-1338	dobersteincl@doj.state.wi.us
Training Officer	Vacant	608-261-5800	608-267-1338	
Training Officer	Patricia Ninmann	608-266-9341	608-267-1338	ninmannpm@doj.state.wi.us
Training Officer	Amy Zabransky	608-264-9452	608-267-1338	zabranskyak@doj.state.wi.us
TIME Systems Operations Manager	Chris Kalina	608-266-7394	608-267-1338	kalinaca@doj.state.wi.us
TIME & *e*TIME Analyst	Mary Moroney	608-266-2426	608-267-1338	moroneym@doj.state.wi.us
TIME & eTIME Analyst	Katie Schuh	608-261-8135	608-267-1338	schuhkr@doj.state.wi.us
TIME & eTIME Analyst	Craig Thering	608-266-7792	608-267-1338	theringcd@doj.state.wi.us
TIME & *e*TIME Analyst	Zach Polachek	608-264-9470	608-267-1338	polachekzd@doj.state.wi.us
TIME & *e*TIME Analyst	Molly Boss	608-266-7955	608-267-1338	bossmk@doj.state.wi.us
Supplies and Imaging	Capri Lione	608-264-6231 608-266-9561	608-267-4558	lioneca@doj.state.wi.us
TIME Billing	Mary Moroney	608-266-2426	608-267-1338	moroneym@doj.state.wi.us
AFIS Operations Manager	Adrianna Bast	414-382-7500	414-382-7507	bastar@doj.state.wi.us
Criminal History Section (Record Check & Criminal Records)	Capri Lione	608-264-6231 608-266-9561	608-267-4558	lioneca@doj.state.wi.us
Firearms Unit	Andrew Nowlan Bradley Rollo	608-267-2776 608-261-8134	608-267-1338 608-267-1338	nowlanam@doj.state.wi.us rollobr@doj.state.wi.us
TRAIN		608-266-7792	608-267-1338	CIBTrain@doj.state.wi.us
Data & Statistics	Derek Veitenheimer	608-266-7185	608-266-6676	veitenheimerdj@doj.state.wi.us
Uniform Crime Reporting (UCR)	Derek Veitenheimer	608-266-7185	608-266-6676	veitenheimerdj@doj.state.wi.us
WIJIS Justice Gateway	Zach Polachek	608-264-9470	608-267-1338	polachekzd@doj.state.wi.us
Interoperability		608-261-7536	608-266-7315	
TSCC		608-266-7633-	608-266-7315	
WILEnet		608-266-8800		wilenet@doj.state.wi.us

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

Resources

Name	Telephone/Website	Terminal Identifier	Email/Fax
National Crime Information Center (NCIC)			
Recalls	304-625-3020		acjis@leo.gov
Hits to Wants	304-625-9245		304-625-9899
International Justice and Public Safety Information Sharing Network (Nlets)			
Control Center	800-528-4020		helpdesk@nlets.org
WI Crime Information Bureau (CIB)			
TIME System Control Center	608-266-7633	TSCC	
Training materials	www.wilenet.org		
Policy & Manuals	www.wilenet.org		
WI Dept of Corrections (DOC)			
Probation & Parole	608-240-3750		
Central Records	888-222-4362		
WI Dept. of Natural Resources (DNR)			
Enforcement	608-266-2141	WDNR	
Registration	608-266-2621	RDNR	
WI Dept. of Transportation			
Vehicle Records	608-266-1466	WREG	
Driver's Records	608-267-1854	WOLN	driverrecords.dmv@dot.state.wi.us
Compliance/Restoration	608-261-0409		
National Center for Missing or Exploited Children (NCMEC)	800-THE-LOST		
	www.missingkids.com	VA007019W	
National Insurance Crime Bureau (NICB)	847-544-7000	ILNICB000	
WI Clearinghouse for Missing & Exploited Children & Adults	800-THE-HOPE		wimissingpersons@doj.state.wi.us
WI Consolidated Court Access (CCAP)	wcca.wicourts.gov		
US I.C.E. Bulk Cash Smuggling Center (BCSC)	866-981-5332	VTICE1600	