

Limited Access v7.2021.3

1.1 Home Page



Notes:

Welcome to the Florida Department of Law Enforcement (FDLE) Criminal Justice Information Services (CJIS) Limited Access Certification Course. Please allot at least one hour to complete this training.

1.2 Introduction



Notes:

A Limited Access user is defined as an operator at any Florida law enforcement/criminal justice agency who only performs queries within the Florida Crime Information Center (FCIC), the National Crime Information Center (NCIC), and the International Justice and Public Safety Network (Nlets).

A Limited Access user's ability to make queries or receive responses described in this certification course may depend on: the job function/assignment the user is performing within the agency; the type of product used to access FCIC/NCIC; and the terminal/device settings and restrictions. A Limited Access user will not be able to make Hot File record entries. Those functions are restricted to Full Access users.

1.3 Criminal Justice Network (CJNet)



Notes:

The Florida Criminal Justice Network, otherwise known as the CJNet, is maintained by FDLE and provides access to state and national criminal justice resources relating to Law Enforcement, Judicial, and Correctional information. The CJNet also offers users secure email services to exchange sensitive criminal justice information, and a calendar that provides information on CJIS training statewide. Access to CJNet is provided only to Florida criminal justice and law enforcement agencies.

1.4 CJNet



Notes:

The CJNet provides access to several criminal justice databases such as FALCON. FALCON is a statewide database which allows for the management of retained applicant fingerprints, the creation of watch lists, and supports the use of Rapid ID devices. Users can utilize the Florida Department of Corrections Offender Information Network for access to Florida prison and probation records. The CJIS Resource Center provides access to frequently used references such as Memorandums, Manuals, and the Training Calendar. Additionally, the CJNet provides access to federal databases which include the Federal Bureau of Prisons where federal inmates can be searched nationwide.

1.5 Florida Crime Information Center (FCIC)

Florida Crime Information Center

FCIC Provides Access to

- ✓ Florida Criminal History Record Information (CHRI)
- ✓ Hot File Records
 - Persons
 - Status
 - Property
- ✓ Florida Concealed Weapon Permits



Notes:

FCIC is the primary system used to access Florida records including Criminal History Record Information (CHRI), and Hot Files which include Person, Status, and Property files. In addition, FCIC also supports queries of Concealed Weapon Permits issued by the Department of Agriculture and Consumer Services. The Concealed Weapon Permit information is provided only to law enforcement agencies.

1.6 National Crime Information Center (NCIC)

National Crime Information Center

Provides access to National Hot Files

- ✓ Wanted Persons
 - ✓ Missing Persons
 - ✓ Unidentified Persons
 - ✓ Person Status Files
 - ✓ Property Files
- 
- ✓ Provides access to Interstate Identification Index (III)


Notes:

NCIC is the primary system used to access national Hot file records. Included among these records are Wanted Persons, Missing Persons, Unidentified Persons, Person Status Files and Property Files. NCIC also allows access to the Interstate Identification Index, or III, which provides for the exchange of Criminal History Record Information between states. NCIC is maintained by the Federal Bureau of Investigation and is available to all 50 states, the District of Columbia, Puerto Rico, the U.S. Virgin Islands, Guam, Canada, and all federal criminal justice agencies.

1.7 International Justice and Public Safety Network (Nlets)

International Justice and Public Safety Network

A gateway that supports communications between states, US territories, federal agencies, Canada and INTERPOL (International Criminal Police Organization)

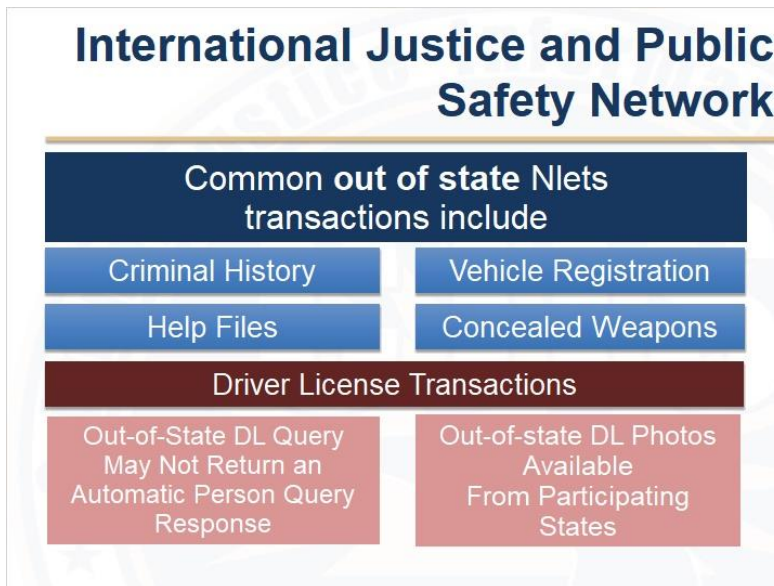


Provides for the interstate/interagency exchange of criminal justice and criminal justice related information over a high-speed message switching system

Notes:

Nlets is a gateway that supports communication between states, U.S. territories, federal agencies, Canada and INTERPOL. The purpose of Nlets is to provide for the interstate and/or interagency exchange of criminal justice and criminal justice related information over a high-speed message switching system. Nlets supports inquiries into each state's motor vehicle, driver's licenses, and criminal history files, as well as other relevant databases.

1.8 Nlets



Notes:

Nlets offers many out of state transaction options. The following is a list of the most commonly used Nlets queries for national information: Criminal History, Vehicle Registration, Help Files, Concealed Weapons, and Driver License Transactions. Please note that unlike an FCIC DL query response, which could include Wanted Person, Missing Person or Status Files information, when a user queries an out of state Driver License through Nlets the user may not receive the automated person responses. Participating states may provide Driver License images with search results. To retrieve available DL images, "Y" must be selected in the Image Request Field of the DL query message key.

Nlets message key GVQ is a VIN Check that provides users with information about a vehicle based on the decoding of the VIN. The VIN Check transaction will leverage data provided by the National Highway Transportation Safety Administration (NHTSA) and will supply users specific vehicle details such as vehicle type, make, model, year and more.

For further information regarding Nlets transactions please visit the Nlets website at www.nlets.org

1.9 CPIC



The graphic is titled "Canadian Police Information Center" in a large, bold, dark blue font. Below the title is a horizontal line. Underneath the line is a dark blue rectangular box with white text that reads: "Canadian Hot File records are not automatically returned with an NCIC query". Below this box is another dark blue rectangular box with white text that reads: "CPIC Nlets Message Keys". Below this box is a grid of six light blue rectangular buttons with dark blue text, arranged in two columns and three rows. The buttons are labeled: "WQ- Persons", "VQ- Vehicles", "CAQ- Articles" in the left column, and "CGQ- Guns", "CSQ- Securities", "CBQ- Boats" in the right column.

Canadian Police Information Center

Canadian Hot File records are not automatically returned with an NCIC query

CPIC Nlets Message Keys

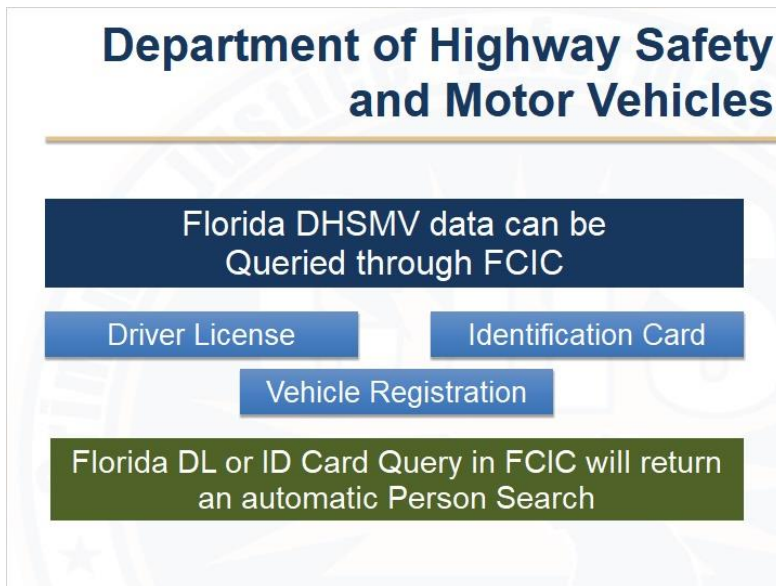
WQ- Persons	CGQ- Guns
VQ- Vehicles	CSQ- Securities
CAQ- Articles	CBQ- Boats

Notes:

Canadian Hot File records are not automatically returned with an NCIC query. However, agencies have the ability to query Canadian entries directly from the Canadian Police Information Centre (CPIC) by using these Nlets message keys.

- WQ for Persons
- VQ for Vehicles
- CAQ for Articles
- CGQ for Guns
- CSQ for Securities and
- CBQ for Boats

1.10 DHSMV



Notes:

Users may query DHSMV data through FCIC, and receive responses from DHSMV, FCIC, NCIC, and perhaps Nlets, depending upon search criteria used. A Florida DHSMV response will be received when a Florida driver license, identification card and vehicle registration query is made using FCIC. An FCIC query of a driver license or identification card by number, or the card holder's full name, will return an automatic person search that may include Wanted Persons, Missing Persons, or Status Files.

1.11 DHSMV

Department of Highway Safety and Motor Vehicles

Use of Emergency Contact Information is
restricted for emergencies

F.S. 119.0712: "Without the express consent of the
person to whom such emergency contact
information applies, the emergency contact
information contained in a motor vehicle record may
be released only to law enforcement agencies for
purposes of contacting those listed in the
event of an emergency"


Notes:

When a response includes Emergency Contact Information (ECI), it should be noted that the use of the ECI is for emergency purposes only and **shall not** be used for investigative purposes per Section 119.0712, Florida Statutes, which states: *"Without the express consent of the person to whom such emergency contact information applies, the emergency contact information contained in a motor vehicle record may be released only to law enforcement agencies for purposes of contacting those listed in the event of an emergency."*

1.12 DHSMV

Department of Highway Safety and Motor Vehicles

When querying specified Florida specialty tags the user is required to enter additional "hidden" characters

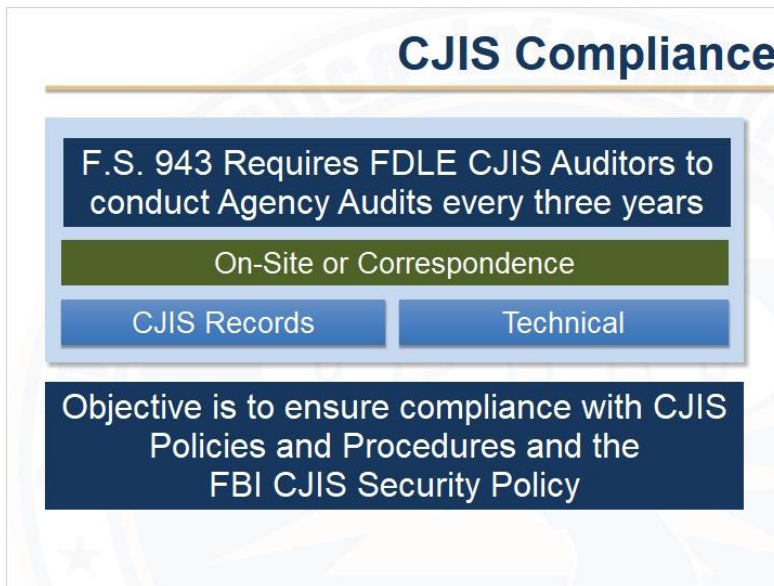


See the Resource Document 'DHSMV - Specialized Tags'

Notes:

When querying Florida vehicle tag information, users are required to enter additional "hidden" characters for certain Florida Specialty Tags. For example, when querying a Purple Heart tag, the user must enter the word HEART immediately preceding the letters and/or digits that appear on the actual tag. Refer to the resource document "DHSMV - Specialized Tags" for further information on how to query these "hidden" character tags. This document can be printed for future reference.

1.13 CJIS Compliance



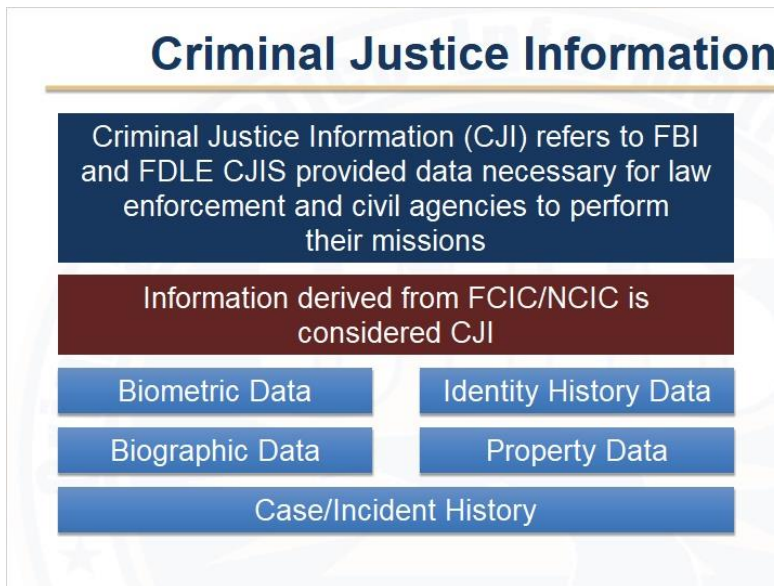
Notes:

In compliance with Florida Statute 943, FDLE CJIS Auditors will conduct either an on-site or correspondence audit on every criminal justice and law enforcement agency that has access to FCIC, NCIC and the CJNet. Agencies will receive a CJIS Records Audit and Technical Audit triennially, or every three years. The CJIS Records Audit and Technical Audit will be conducted at different times as established by the auditor and the agency.

The objective of the audits is to ensure compliance with the CJIS Policies and Procedures and FBI CJIS Security Policy. These guidelines must be adhered to in order for the agency to maintain FCIC and NCIC access.

The information provided in this Limited Access training includes policies and procedures you as a user must adhere to in order for your agency to be operating in compliance.

1.14 Criminal Justice Information



Notes:


Criminal Justice Information, or CJI, is the term used to refer to all of the FBI/FDLE CJIS provided data that is necessary for law enforcement, criminal justice, and statutorily authorized agencies to perform their missions. Any information that is derived from FCIC or NCIC is considered CJI, is protected data, and must be treated accordingly.

CJI includes Biometric Data which is used to uniquely identify individuals from within a population; Identity History is textual data that corresponds with a subject's biometric data, providing history of criminal and/or civil events; Biographic Data is information about subjects associated with a unique case, and not necessarily connected to identity data; Property Data is information about vehicles and property associated with a crime; and Case or Incident History includes information about the history of criminal incidents.

1.15 Personally Identifiable Information

Personally Identifiable Information

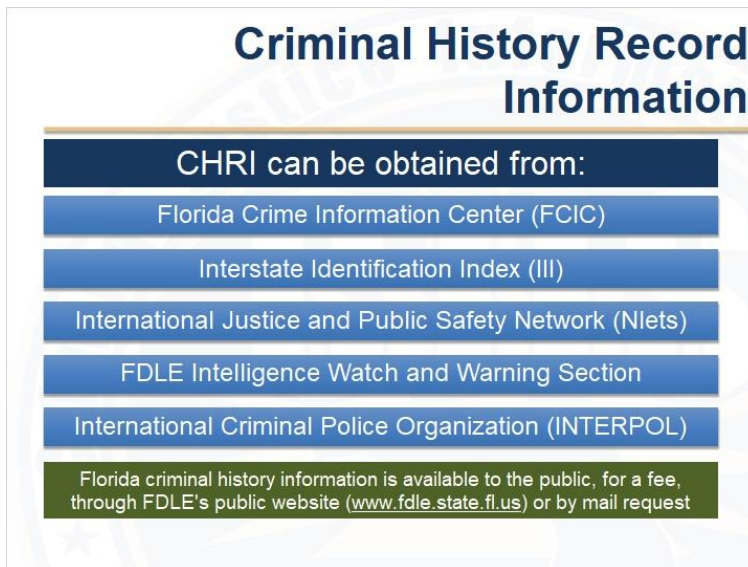
- ✓ PII is information used to distinguish or trace a person's identity
 - Name
 - Social Security Number (SSN)
 - Biometric records
- ✓ PII may include information that is used alone or combined with other personal or identifying information
- ✓ PII shall be extracted from CJI for the purpose of official business only



Notes:

Personally Identifiable Information, or PII, is information that can be used to distinguish or trace a person's identity such as name, social security number or biometric records. PII may include information that is used alone or combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth or mother's maiden name. PII shall be extracted from CJI for the purpose of official business only.

1.16 Criminal History Record Information (CHRI)



Notes:

Criminal History Record Information, or CHRI, is available from multiple sources, and it may be necessary to make more than one query to obtain an individual's complete criminal history. Criminal history queries into FCIC will return only arrests in the state of Florida, while an NCIC III query will return arrest information from other states and federal agencies. Additionally, Nlets provides direct access to a state's criminal history repository, allowing a user to query CHRI directly from the state of record.

Agencies may also submit a request with the FDLE Intelligence Watch and Warning Section to acquire CHRI on persons from another country. The Watch and Warning Section will contact the International Criminal Police Organization (INTERPOL) for assistance and is the only agency in Florida that can request CHRI from INTERPOL. The Watch and Warning Desk can be contacted by phone, (850) 410-7645, or by email, FloridaFusionCenter@fdle.state.fl.us


In December 2019 the FCIC message switch began generating an INTERPOL Person Query (IPQ) for qualifying Florida Driver Queries (FDQ) and Wanted Persons Queries (QW). INTERPOL's data includes international alerts and advisories on persons who are wanted for prosecution or to serve a sentence; are missing; are of interest in an active criminal investigation, or are considered a threat to public safety, based on their prior criminal history. Response should be examined very carefully to confirm that the response is the same subject. For more information see CJIS Memo 2019-16.

Finally, the public may obtain Florida criminal history information, for a fee, by visiting FDLE's public website at www.fdle.state.fl.us.

1.17 Criminal History Record Information (CHRI)

Criminal History Record Information

- ✓ CHRI is "restricted data" and is a subset of CJI
- ✓ Shall be accessed only for an authorized purpose
- ✓ Dissemination of CHRI
 - The other agency is an Authorized Recipient
 - The other agency is performing personnel appointment functions for criminal justice applicants



Notes:

CHRI is "restricted data", is a subset of CJI, and contains arrest, judicial, and sentencing information. The confirmation of the existence of a Computerized Criminal History (CCH) or the nonexistence of a CCH, is considered to be dissemination of CHRI. Due to the sensitivity of the information contained in CHRI, additional controls are required for the access, use and dissemination of CHRI. CHRI shall only be accessed for authorized purposes and shall only be used for the purpose for which it was accessed.

The dissemination of CHRI to another agency is allowed if the other agency is an authorized recipient of such information and is being serviced by the accessing agency and/or the agency is performing personnel appointment functions for criminal justice employment applicants.

1.18 Criminal History Record Information (CHRI)

Criminal History Record Information

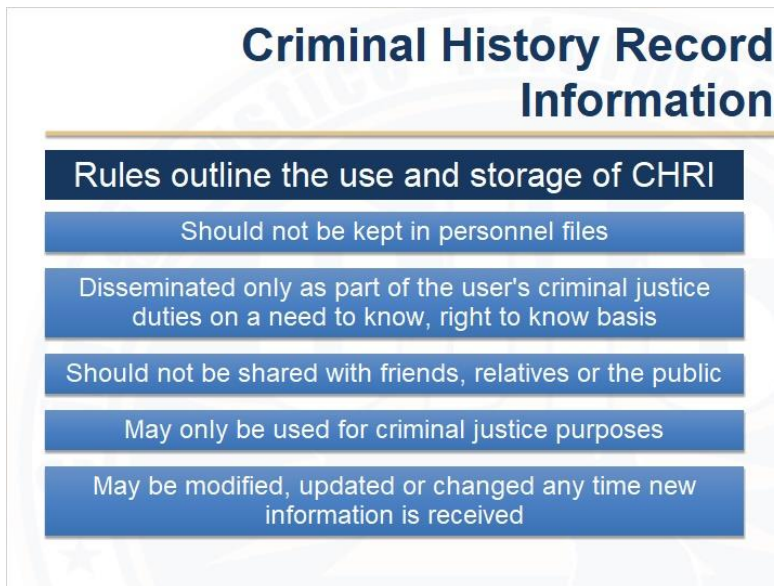
- ✓ Used by law enforcement and criminal justice agencies for official purposes only
- ✓ Some non-criminal justice agencies have access to CHRI data as outlined in Florida Statute or federal regulation
- ✓ Voice transmissions (radio) should be limited to what is needed for officer or public safety
- ✓ CHRI should not be emailed through non-secure means, however it may be faxed to agencies allowed to receive the information
- ✓ Non-compliance due to lack of knowledge and system functionality is not acceptable

Notes:

CHRI should only be used by law enforcement and criminal justice agencies for official criminal justice purposes only. Additionally, some non-criminal justice agencies are allowed access to CHRI based upon Florida statute or by Federal regulation. Due to the confidential nature of CHRI, voice transmission over a radio should be strictly limited to what is immediately needed to ensure officer or public safety.

CHRI should never be emailed over a non-secure network. If faxing CHRI, the receiving agency must be authorized to receive the information and the information must be sent via a phone line or secure network. Users must ensure they understand what information is returned and how to query CHRI properly in the software application used to access FCIC and NCIC; and users must have a clear knowledge of what Purpose Code to use for the CHRI being queried. Non-compliance due to lack of knowledge and system functionality is not acceptable.

1.19 Criminal History Record Information (CHRI)



Notes:

There are rules outlining the use and storage of CHRI data. CHRI should not be kept in personnel files because those files may become public record. The dissemination of CHRI is on a need to know, right to know basis and should never be shared with friends, relatives or the public. Querying or sharing CHRI for anything other than criminal justice related duties constitutes a violation of user privileges and specified state and national laws. The CHRI is constantly changing and may be modified, updated, or changed any time new information is received; therefore, a new CHRI query must be made each time a subject's record is under review.

1.20 Criminal History Record Information (CHRI)

Criminal History Record Information

Specified National Status File Records are also to be treated as CHRI

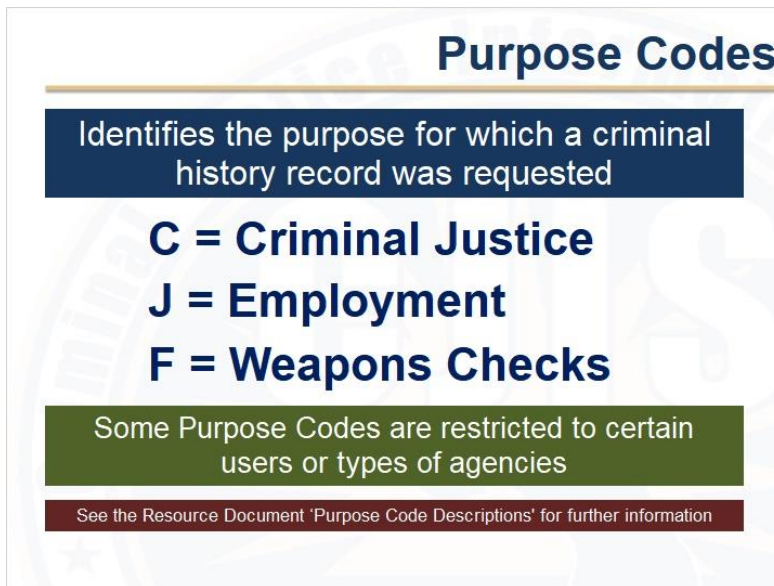
- ✓ Gang Files
- ✓ Known or Appropriately Suspected Terrorist Files
- ✓ Supervised Released Files
- ✓ National Sex Offender Registry Files
- ✓ Historic Protection Order Files of NCIC
- ✓ Identity Theft Files
- ✓ Protective Interest Files
- ✓ Person with Information data in the Missing Person File
- ✓ Violent Person Files
- ✓ NICS Denied Transaction Files

Notes:

In addition to CHRI being restricted data, the FBI CJIS Security Policy also requires some specified National Status File records to be treated as CHRI. These restricted Status Files must be treated consistent with the access, use and dissemination of CHRI data. These restricted files include:

- Gang Files
- Known or Appropriately Suspected Terrorist Files
- Supervised Released Files
- National Sex Offender Registry Files
- Historic Protection Order Files of NCIC
- Identity Theft Files
- Protective Interest Files
- Person with Information data in the Missing Person File
- Violent Person Files
- NICS Denied Transaction Files

1.21 Purpose Codes

A graphic titled "Purpose Codes" with a background of a faint circular seal. It contains four colored boxes with text: a dark blue box at the top stating the purpose of the codes, a list of codes (C, J, F) in bold blue text, a green box stating some codes are restricted, and a small dark red box at the bottom pointing to a resource document.

Purpose Codes

Identifies the purpose for which a criminal history record was requested

C = Criminal Justice
J = Employment
F = Weapons Checks

Some Purpose Codes are restricted to certain users or types of agencies

See the Resource Document 'Purpose Code Descriptions' for further information

Notes:

Purpose Codes are used to identify the purpose for which a criminal history record was requested. The appropriate Purpose Code must be used when querying a criminal history record. Purpose Code C is used for criminal justice purposes, including site security and investigations. Purpose Code 'J' is used for employment background checks; it should not be used for site security checks. Purpose Code 'F' is used for weapons checks, including returning a lost or recovered firearm to the owner.

Some Purpose Codes are restricted to certain users or types of agencies. Users should only use Purpose Codes approved for their specific agency, FCIC/NCIC terminal, or authorized purpose. Refer to the resource document "Purpose Code Descriptions" for further information on the proper use of Purpose Codes.

1.22 Use of Data

Use of Data

CJI, PII and CHRI can only be used/disseminated in the administration of criminal justice duties

Users should be aware that improper handling and sharing of CJI, PII and CHRI could result in criminal prosecution

Notes:

The CJI, PII and CHRI can only be used and/or disseminated in the administration of criminal justice duties. Users should be aware that the improper handling and sharing of CJI, PII and/or CHRI could result in criminal prosecution.

1.23 How a Florida Criminal History is Created



Notes:

Do you know how a criminal history record is created? First, an individual is arrested and then taken to the booking facility to be fingerprinted on a digital fingerprint device also known as a Livescan device. Next, the fingerprints are electronically sent and compared against Florida fingerprint records from previous arrests to determine if a past history exists for the subject. If no prior arrest exists, the subject is automatically assigned a Florida State Identification (SID) Number and the arrest is added to the criminal history file. If a prior arrest exists, the new charge is added to the existing record of the subject.

Florida Criminal History

--FLORIDA CCH RESPONSE--
FS.DLE/03999999.PUR/CATN/
SID NUMBER: 03999999 PURPOSE CODE: Criminal Justice

----- IDENTITY SECTION -----

State ID
03999999

FBI Number 57802SDC5	DOC Number K99999
-------------------------	----------------------

----- DEMOGRAPHICS -----

Name FLORIDA, TEST RECORD	Date of Birth 08/24/1984	Social Security Number 933-39-9999
------------------------------	-----------------------------	---------------------------------------

Sex Male	Race White	Place of Birth Georgia
Height 5' 10"	Weight 150 lbs	Ethnicity
Hair Color Black	Eye Color Green	

Other Name(s)
TEST, RECORD
CRB, TEST RECORD
Record, Test

Other Date(s) of Birth 08/23/1984	Other Social Security Number(s) 933-99-9999 939-99-9999
--------------------------------------	---

Miscellaneous Numbers(s)
Air Force Serial-5986542

Address
1234 MAIN STREET, TALLAHASSEE, Florida

Scars Marks Tattoos
FOREHEAD
CHEEK, RIGHT

Elements of a criminal history include personal identifiers such as name, race, sex, date of birth, social security number, state identification number, FBI number, miscellaneous numbers as well as alias information and other personal descriptors.

1.25 Florida Criminal History

Florida Criminal History

===== Cycle 1 =====

OBTS 9876543210

** Sealed pursuant to Florida Statute(s) 943.059 **

Arrest

Date of Arrest 01/10/1998

Charge 001

Arresting Agency ORI FL0130000

Arresting Agency Name MIAMI DADE County Sheriffs Office/PD

Agency Case Number 12123

AON Description Possession Of Weapon

Statute	Level	Degree
	Unknown	Unknown

Charge Count 1

Charge 002

Arresting Agency ORI FL0130000

Arresting Agency Name MIAMI DADE County Sheriffs Office/PD

Agency Case Number 12123

AON Description Carrying Concealed Weapon

Statute	Level	Degree
	Unknown	Unknown

Charge Count 1

Charge 003

Arresting Agency ORI FL0130000

Arresting Agency Name MIAMI DADE County Sheriffs Office/PD

Agency Case Number 12123

AON Description Forgery Of Checks-

Statute	Level	Degree
	Unknown	Unknown

Charge Count 1

If further information is desired please contact FL03701C1 via Administrative Message or call 1-850-410-7870 between the hours of 0800-1700 M-F.

Notes:

CHRI elements include arrest(s), disposition(s), and sentencing information. Additionally, information on criminal registration(s), sexual predator and offender registration(s), and clemency may also be included in the CHRI.

1.26 Attention Field

Attention Field
Mandatory Field for Criminal History Request
Must include the name of the requestor to uniquely identify the requestor
Include badge number, case number or other specific data - Inv Johnson, badge #12309 - Ofc Roberts, radio #123
Include agency name if request is from an authorized external agency

Notes:


The Attention Field is mandatory and must contain the name of the person requesting the CHRI, to uniquely identify the requestor of the CHRI. In addition to the requestor's name, a badge number, case number or other specific data should be included to assist in identifying the requestor and the purpose of the request. Including citation, case, or computer aided dispatch numbers as well as the agency name, if the request is from an authorized external agency, is suggested.

1.27 Secondary Dissemination

Secondary Dissemination

When a user shares any part of CHRI, physically or verbally, with another criminal justice professional outside his/her agency

- ✓ Includes disclosing the fact that a query was run and no criminal history was found



Notes:

Secondary Dissemination occurs when the person requesting and/or in the possession of the criminal history shares any part of that information, physically or verbally, with another criminal justice professional outside of his/her agency. Confirming or denying the existence of Criminal History Record Information is considered Secondary Dissemination and should be documented on the Secondary Dissemination Log.

1.28 Secondary Dissemination Log

Secondary Dissemination

Date	Subject's Name	SID or FBI Number	Requestor (released to)	Requestor Agency (released to)	Operator (released by)	Reason Disseminated	Purpose Code
3/3/2012	Public, Carl	FL01198577	Detective Smith	Broward County Sheriff's Office	Investigator Jones	Investigation	C

Document the sharing of CHRI on the Secondary Dissemination Log

Sharing is verbally or physically

Handwritten or electronic format

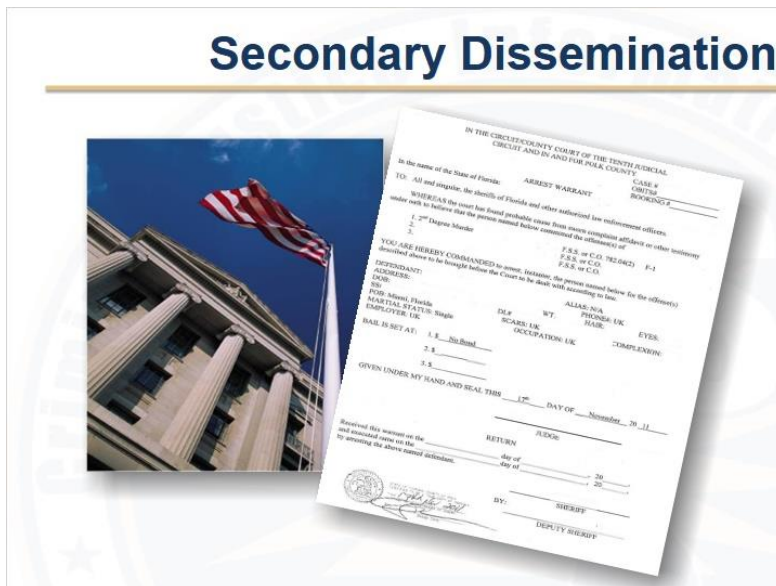
Must be maintained at the agency for at least four years

For a sample Secondary Dissemination Log, see the Resource Document 'Sample Secondary Dissemination Log'

Notes:

Personnel must document the sharing of CHRI on a Secondary Dissemination Log. Disseminating criminal history data means the person in possession of the history shares it, verbally or physically, with an authorized agency member outside of the user's agency. The person sharing the CHRI could be the person that ran the history, or it could be a person who had the history run for them by another operator. Secondary Dissemination Logs can be handwritten or in electronic form and must be maintained at the agency for at least four (4) years. These logs are required and must contain the information listed. For a sample Secondary Dissemination Log, see the resource document 'Sample Secondary Dissemination Log'.

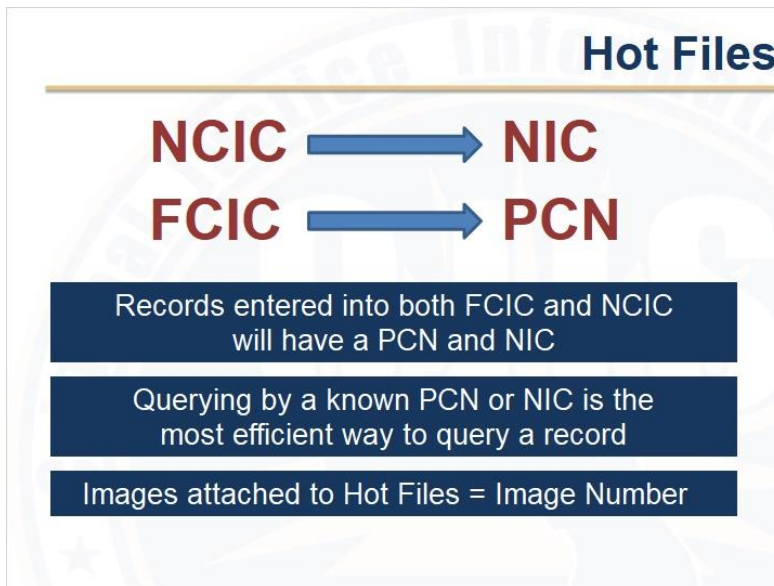
1.29 Secondary Dissemination



Notes:

Consider this...You are an investigator obtaining a warrant on a suspect in a homicide case. The process requires CHRI to be provided to the State Attorney's Office, the Clerk of the Court and the Judge. Once the CHRI leaves your hands and is given to the State Attorney's Office, the Clerk of the Court and the Judge, it becomes secondary dissemination. This means the CHRI dissemination must be logged in a Secondary Dissemination log, kept at your agency for four years and made available during your agency's CJIS audit.

1.30 Hot Files



Notes:

As records are entered into NCIC, the system automatically generates and attaches an NCIC number or NIC. The NIC is randomly assigned by NCIC and indicates the specific file in which the record is contained. As records are entered into FCIC, the system automatically generates and attaches a Process Control Number or PCN. Likewise, the PCN is randomly assigned by FCIC and indicates the specific file the record is contained in.


Records that are entered into both the FCIC and NCIC systems will have a PCN and a NIC assigned to the record. A known PCN or NIC is the most efficient way to query a record. Additionally, a Hot File response may contain an image which is assigned an Image Number by NCIC. Images that are not automatically displayed may be queried specifically by each individual Image Number.

1.31 Hot Files

Hot Files

Records entered into FCIC/NCIC by an agency upon receiving notification that

- ✓ A Person reported as Wanted, Missing or Unidentified
- ✓ Property in question has been reported Stolen, Abandoned, Lost or Recovered
- ✓ Entries must have supporting documentation
- ✓ Files are constantly being updated



Notes:

Hot Files are records entered into FCIC/NCIC by an agency upon receiving notification that a person is wanted, missing or unidentified or property in question has been reported stolen, abandoned, lost or recovered. Agencies must have supporting documentation for all entries placed in the FCIC and NCIC systems. Supporting documentation includes reports, supplemental documentation, and images. All files are constantly being updated; therefore, the entry is only current at the time of query.

1.32 Property Files Introduction



Notes:

Property files include the following records: Articles, Guns, Vehicles, Boats, Vehicle and Boat Parts, and Securities. The Property File consists primarily of stolen items; however, some exceptions exist in specific files. Property must be uniquely identifiable by a serial number or other permanent identifying number to be contained within the hot files. When querying the property files, the user must make the query into the specific file of interest to get the correct response.

1.33 Property Files



Notes:

The Article File contains miscellaneous property other than boats, guns, vehicles and securities. In addition to stolen items, an article file query may return information on lost items of identification and property belonging to and/or associated with public safety, homeland security and critical infrastructure. Records regarding stolen toxic, hazardous materials are also available in the Article File. When making a query into the Article File, if the Type Field category code is not known, entering the identical Serial Number or Owner Assigned Number (OAN) in the appropriate field, and placing a Y in the Type Field, will return a hit regardless of the Type Field code used in the entry.

The Gun File contains weapons that expel a projectile by air, carbon dioxide, or the action of an explosive. Some exceptions are BB, paintball, pellet and air soft guns, which are entered in the Article File rather than the Gun File. Gun serial numbers are not unique, so responses should be carefully reviewed to ensure the make, model and caliber match the queried gun before taking any action. Gun file responses will return information on stolen, lost, and recovered guns.

The Securities File includes records of currency, stocks, bonds and other financial instruments that have a denominational value and a unique identifying number. Responses may return information on securities that have been reported as stolen, embezzled, used for ransom or counterfeited.

1.34 Property Files



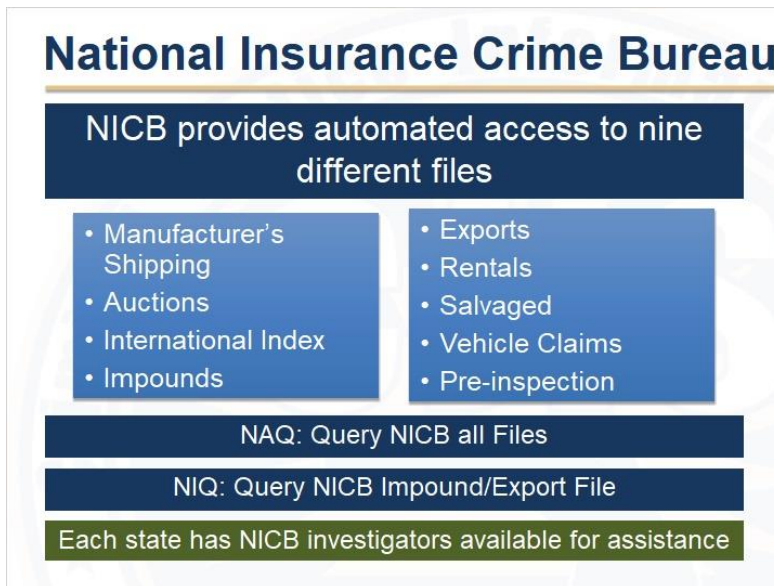
Notes:

Vehicle File queries return information on stolen vehicles, aircraft, trailers, construction equipment, farm and garden equipment, license plates, and vehicle and boat parts. These queries will provide responses regarding stolen, abandoned, and felony vehicles. A query into the Vehicle File, and a query into the Vehicle Registration File, are two different transactions and performed differently for in-state and out-of-state vehicles.

Boat queries return information on stolen boat entries. Additionally, a query into the Boat File, and a query into the Boat Registration File, are two different transactions. When querying Nlets out of state Boat Registration (BQ) information, the registration state's postal abbreviation is often a part of the information entered into the boat registration field. There are some states that have an alternate postal abbreviation that must be used when making this query. These abbreviations are different than the state's postal abbreviation. See the resource document 'Boat Registration Query' for further information.

A Part is defined as any serially-numbered component from a vehicle or boat. Examples of parts or attachments for a vehicle or boat include an engine, wheels, battery, outboard motor or items used in conjunction with vehicles such as an automobile battery charger, tow bar, or certificate of title.

1.35 NICB



Notes:

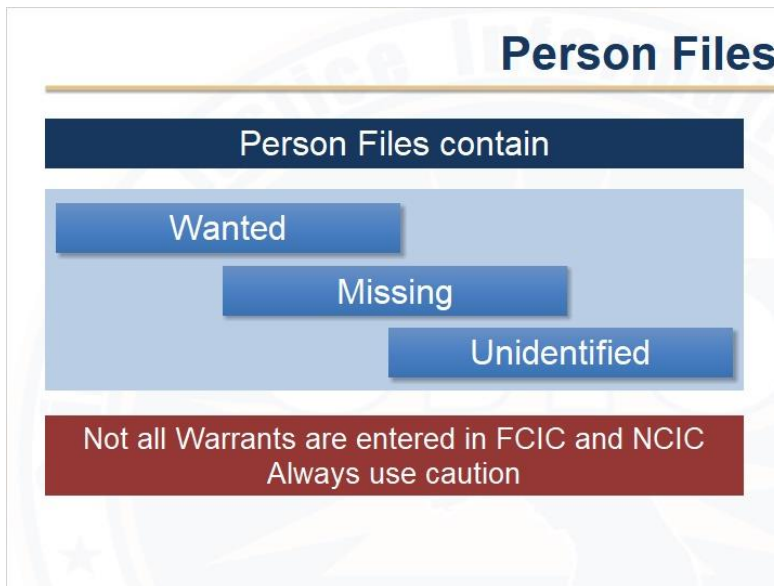
The National Insurance Crime Bureau (NICB) provides automated access to nine different files:

- Manufacturer's Shipping
- Auctions
- International Index
- Impounds
- Exports
- Rentals
- Salvaged
- Vehicle Claims
- Pre-inspection

The NICB Files message key 'NAQ: Query NICB all Files', accesses all nine listed files, while the 'NIQ: Query NICB Impound/Export File', only queries Impound and Export Files. Access to these files is for investigative purposes only.

Additionally, NICB investigators are available to assist agencies with identifying vehicle make and model from surveillance videos, conduct offline searches of old purged stolen vehicle records, conduct color code searches, and determine the color of a vehicle by the VIN. Each state has NICB investigators available for assistance. For more information, visit the NICB website at www.nicb.org

1.36 Person Files



Notes:

Person file queries will return information on Wanted, Missing and Unidentified Person Records. It is important to note that not all issued warrants are entered into the Wanted Person File. Some agencies only enter felony warrants and high-level misdemeanors, while some agencies enter all warrants. Sworn personnel should take this into consideration as an officer safety issue.

1.37 Person Files

Person Files

Wanted Persons

- ✓ Outstanding Warrants
- ✓ Probation or Parole Violators
- ✓ Escapees
- ✓ Temporary Felon
 - When an agency is in the process of obtaining a felony warrant and prompt action must be taken to apprehend individual
- ✓ Wanted Person's Query may return
 - Subjects stolen driver license, social security number, or miscellaneous number if entered in the Article File
 - Subjects entered in NDTF for denial of firearms purchase

Notes:

Wanted Person Files include any individual, including a juvenile who will be tried as an adult, for whom a federal, felony or serious misdemeanor warrant is outstanding, individuals that are probation and parole violators, and escapees.

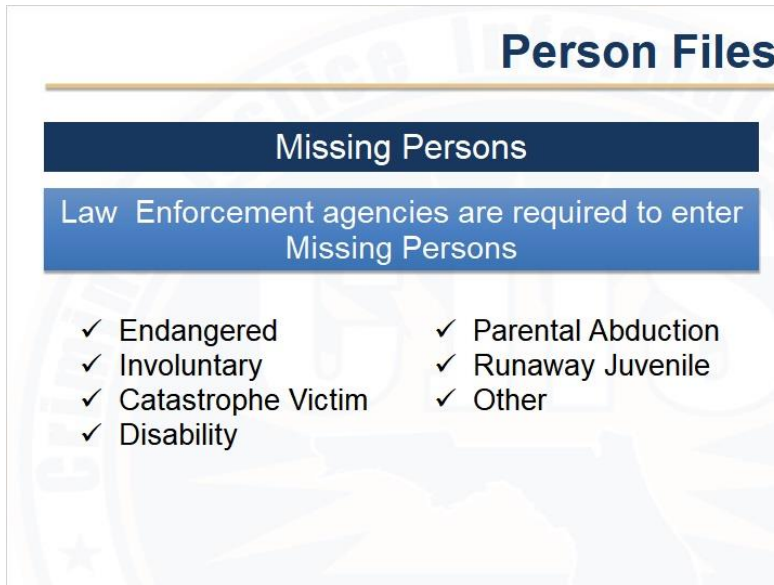
Temporary Felon records are also contained within the Person Files. A Temporary Felon record contains information on a person an agency is in the process of acquiring a felony warrant on, and determines the subject may flee; therefore, prompt action must be taken to apprehend the individual. Temporary Felon records are automatically purged 48-hours after entry.

When running a Query Wanted (QW) transaction, if the subject's driver license, social security number or miscellaneous number is also queried, a cross search of the Article File will be conducted. If identification documents such as DL cards, Social Security cards, or others containing a specific number are entered into the Article File (like a military ID card, a Visa or passport, etc.), those hits will be returned as part of the response to the QW query if the identifying number is included with a Person File entry.

Subjects that have been entered in the National Instant Criminal Background Check System (NICS) Denied Transaction File (NDTF) for denial of firearms purchase may be returned with a QW transaction. The knowledge of the denial of prohibited persons will alert the user to the subject's tendency to possess, attempt to possess, or use of firearms. This awareness may suggest a host of possible actions or precautions that law enforcement or criminal justice agencies

may want or need to take during their encounter with the subject. With the additional data, the search results may include multiple hits to the subject/detainee spanning six months.

1.38 Person Files



Person Files

Missing Persons

Law Enforcement agencies are required to enter Missing Persons

- ✓ Endangered
- ✓ Involuntary
- ✓ Catastrophe Victim
- ✓ Disability
- ✓ Parental Abduction
- ✓ Runaway Juvenile
- ✓ Other

Notes:

According to Florida Statute 937.021, law enforcement agencies are required to enter persons that are reported as missing into FCIC/NCIC. A Missing Person Record can be entered for an adult or juvenile, and must be categorized as endangered, involuntary, catastrophe victim, disability, parental abduction, runaway juvenile, or other.

In the absence of documentation from a parent, legal guardian, next of kin, physician, or other authoritative source, including a friend or neighbor in unusual circumstances, or when such documentation is not reasonably attainable, a signed missing person report by the investigating officer, is permissible.

1.39 Person Files

Person Files

Missing Persons

Person With Information (PWI)

- ✓ Supplemental record attached to an endangered or involuntary missing person record
- ✓ Indicates that an individual may have information regarding the missing person
- ✓ PWI responses will include 'Warning - Do not arrest based on this information alone'

INTERPOL has the authority to enter records on abducted children and other missing persons from other countries

--FCIC HIT RESPONSE--
#NIC HIT (9884)

WARNING - DO NOT ARREST BASED ON THIS INFORMATION ALONE

MISSING PERSON ENDANGERED

THIS RECORD INCLUDES PERSON WITH INFORMATION DATA.

NAME: GINNY TEST	LAST CONTACT: 05/09/2019
DOB: 19890627	ENTRY DATE: 05/11/2019
RACE: WHITE	PCN: T200090475
SEX: FEMALE	NIC: M35000579
HEIGHT: 506	
WEIGHT: 120	
HAIR COLOR: BROWN	
EYE COLOR: BLUE	
MNP: MP	
CASE NO: ABCD1234	
ENTERING MNE: D37010095	
ENTERING AGY: FL0370156 - FDLE - TALLAHASSEE	
NOTIFY AGY: NO NOTIFY PUBLICLY AVAILABLE	

PERSON WITH INFORMATION

NAME: JOHNNY TEST	ENTRY DATE: 05/11/2019
DOB: 19790101	
RACE: WHITE	
SEX: MALE	
CASE NO: ABCD1234	
ENTERING MNE: D37010095	
ENTERING AGY: FL0370156 - FDLE - TALLAHASSEE	
NOTIFY AGY: NO NOTIFY PUBLICLY AVAILABLE	
MSC: THIS PERSON MAY HAVE INFO ON MP-A TEST	

Notes:

A Person With Information (PWI) File may be attached as a supplement to an endangered or involuntary Missing Person File indicating that an individual may have information regarding the location or circumstances related to the Missing Person. PWI responses will include a 'Warning - Do not arrest based on this information alone' banner.

Additionally, the INTERPOL has the authority to enter records on abducted children and other missing persons from other countries when evidence exists indicating that the subject is now in the United States.


1.40 Person Files

Person Files

Unidentified Persons

Includes

- ✓ Deceased
- ✓ Living
- ✓ Catastrophe Victims
- ✓ Body Parts



NCIC conducts Automatic Cross Search with Missing Person Records daily

Notes:

According to Florida Statute 406.145, if a body is not immediately identified, the law enforcement agency responsible for investigating the death is required to complete an Unidentified Person Report and enter the data into the Unidentified Person File in NCIC. The Unidentified Person File is an NCIC-only file and contains information on persons that are deceased, living, or catastrophe victims, as well as body parts.

When an Unidentified Person record is entered or modified, NCIC automatically compares the data in that record against all Missing Person Records. These comparisons are performed daily on the records that were entered or modified on the previous day, and each of the entering agencies are notified of a possible match.

1.41 Person Files

Person File Responses

Responses may include any or all of the records contained in the Person File (Wanted, Missing and Status)

Search is expanded or narrowed based on data and information entered as search criteria

Carefully review all responses received; responses may not match the person searched

See the Resource Document 'Best Practices for Person Searches' for further information

Notes:

When a user queries a Person File, they may receive responses from any or all record types contained within the Person File. For example, a single query may return Wanted, Missing and Status File records.

Responses will vary based on the search criteria used, and the responses may or may not pertain to the individual that was queried; therefore, users are encouraged to perform a thorough review of all responses received. While making a query to the person file, the more information included in the query the narrower the results, while limited information will provide a broad set of responses.

See the resource document “Best Practices for Person Searches” for further information on person queries.

1.42 Status Files

Status Files

WRIT OF BODILY ATTACHMENT STATUS

WARNING - THE FOLLOWING RECORD CONTAINS EXPIRED LICENSE PLATE DATA. USE CAUTION. CONTACT ENTERING AGENCY TO CONFIRM STATUS.

NAME: TEST, VINNY WARRANT DATE: 01/02/2010
DOB: 19600606 ENTRY DATE: 01/06/2010
RACE: WHITE VALIDATED: 02/06/2012
SEX: MALE PCN: T110885525

LIC PLATE: ABC123 LIC ST: FL LIC YR: 2011
NIC: NONE
LIC TYPE: REGULAR PASSENGER AUTOMOBILE PLATES
ORIG OFFENSE: NEGLECT CHILD
WARRANT NO: PURGE AMOUNT: 1800
CASE NO: TESTPENS01
ENTERING MNE: D17890011
ENTERING AGY: FL0170301 - FDLE - PENSACOLA
REGIONAL OPERATIONS CENTER
NOTIFY AGY: NO NOTIFY/NOT PUBLICLY AVAILABLE
--END--

- ✓ Status Files may be returned in addition to the Wanted and Missing Person responses
- ✓ Records are for informational purposes and should be carefully reviewed
- ✓ Violations could result in an arrest

Notes:

When conducting a person query, Status Files may be returned in addition to the Wanted and Missing Person responses. Most Status File records contain a caveat at the beginning of the response indicating that the information is for informational purposes only. However, violations of certain conditions of specified Status File records could result in an arrest such as Writs of Bodily Attachment for failure to pay child support.

1.43 FCIC-Only Status Files

FCIC-Only Status Files

- ✓ High Risk Sex Offender (HRSO)
- ✓ Violent Felons of Special Concern (VFOSC)
- ✓ Florida Inmate Release/Florida Early Release
- ✓ Career Offenders
- ✓ Florida Gang Records
- ✓ Writs of Bodily Attachment
- ✓ Florida Deported Alien
- ✓ Behavioral Threat and Management (BTAM) criteria of the Violent Person File

CRIMINAL GANG MEMBER (FLORIDA STATEWIDE INTELLIGENCE SYSTEM - IN SITE)

STANDING ALONE, THIS INFORMATION DOES "NOT" ESTABLISH PROBABLE CAUSE TO SEARCH OR SEIZE. THIS RECORD DOES INDICATE THAT THIS PERSON IS A MEMBER OF A CRIMINAL GANG PURSUANT TO CHAPTER 874.03, FLORIDA STATUTES.

FLORIDA KNOWN GANG MEMBER STATUS RECORD

WARNING - THE FOLLOWING RECORD CONTAINS EXPIRED LICENSE PLATE DATA. USE CAUTION, CONTACT ENTERING AGENCY TO CONFIRM STATUS.

NAME: TEST TESTER START OF STATUS DATE: 01/01/2019
DOB: 19330303 PCN: T200090982
RACE: BLACK NIC: NONE
SEX: MALE
SOC SEC NO: 000000000
LIC PLATE: 123INTEL LIC ST: FL LIC YR: 2000
LIC TYPE: REGULAR PASSENGER AUTOMOBILE PLATE
VIN: WDCYC7BF9BX00007 VEH YEAR:
CASE NO: 24854
ENTERING MNE: D37010081
ENTERING AGY: FL0370142 - FDLE - TALLAHASSEE
NOTIFY AGY: NO NOTIFY/PUBLICLY AVAILABLE

Notes:

FCIC-Only Status Files are records that are solely provided to Florida agencies. These include High Risk Sex Offenders (HRSO), Violent Felons of Special Concern (VFOSC), Florida Inmate Release and Florida Early Release, Career Offenders, Florida Gang records, Writs of Bodily Attachment, the Florida Deported Alien File, and the Behavioral Threat and Management File of the Violent Person File. These records will only have a PCN assigned.

1.44 NCIC-Only Status Files

NCIC-Only Status Files

Provided to all agencies accessing NCIC

✓ Foreign Fugitive	✓ National Sex
✓ Immigration Violator	Offender Registry*
✓ Federal Supervised Release*	✓ NCIC Gang File*
✓ Identity Theft*	✓ Protective Interest*
✓ National Instant Criminal Background Check System (NICS) Denied Transaction File*	✓ Violent Person File*
	✓ Known or Appropriately Suspected Terrorists (KST)*

Notes:


NCIC-Only Status Files are provided to all agencies accessing NCIC. These files include Foreign Fugitive, Immigration Violator, Federal Supervised Release, Identity Theft, National Instant Criminal Background Check System (NICS) Denied Transaction File, National Sex Offender Registry, NCIC Gang file, Protective Interest, Violent Person File, and the Known or Appropriately Suspected Terrorists or KST file. It is extremely important to note that any KST file responses received from the Terrorist Screening Center must be carefully reviewed and contact must be initiated based upon the instructions contained in the response. These NCIC records will only have a NIC.

Additionally, the status files marked with an asterisk are considered CHRI and should be treated as restricted data and not shared or disseminated publicly or over the radio unless officer or public safety is an issue.

1.45 Status Files in both FCIC and NCIC

Status Files in Both FCIC and NCIC

- ✓ Sexual Predators/Sexual Offenders
- ✓ Protection Orders (both active and historical)
- ✓ Florida Department of Corrections Probation/Parole records



Notes:

Status Files contained in both FCIC and NCIC include the Sexual Predator/Offender File, Protection Orders (which remain in a historical file for five years after being cleared in FCIC/NCIC), and the Florida Department of Corrections Probation and Parole records. These records will have both a PCN and a NIC assigned.

1.46 Jordan's Law

HB 43: Jordan's Law

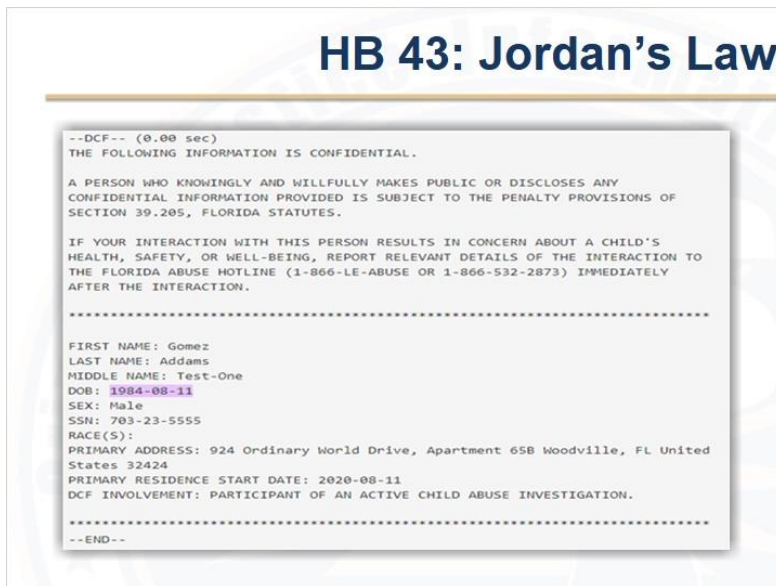
- ✓ Provides Law Enforcement Agencies with DCF Investigative Information
- ✓ FQCP Message Key
- ✓ Demographic Information Needed to Query:
 - ✓ First and Last Name and DOB OR
 - ✓ Social Security Number

Notes:

In support of the passage of House Bill (HB) 43, known as Jordan's Law, an FCIC query has been established to provide law enforcement officers the ability to check if a person is a parent or caregiver of a child who is currently the subject of a Florida child protective investigation for alleged child abuse, abandonment, or neglect, or is a parent or caregiver of a child who has been allowed to return or to remain in the home under judicial supervision after an adjudication of dependency.

The FCIC message key, Florida Query Child Protection (FQCP), allows law enforcement to query the Department of Children and Families (DCF) system and receive a response indicating whether or not the individual is part of a DCF investigation. In order to perform the query, the First name, Last name, and Date of Birth (DOB) OR the Social Security Number of the individual in question must be submitted.

1.47 Jordan's Law



Notes:

A caveat at the top of the message will be provided on every response initiated by this query. Note that the disclosure of the confidential information is subject to penalties.


The last sentence in the response will vary depending upon the circumstances of the child. The two different statements a user may see regarding DCF Involvement include 'DCF Involvement: Participant of an active child abuse investigation.' OR 'DCF Involvement: Parent/Caregiver of Child(ren) Currently Under In-home Supervision.'

If a law enforcement officer is concerned about a child's health and safety, they shall reach out to the Florida Abuse Hotline number 1-866-235-2873 which is also provided within the caveat of the response.

1.48 Identity Theft

Identity Theft File

- ✓ Agency creates victim profile in the Identity Theft File
- ✓ Includes information such as victim name, DOB, SSN, and type of identity theft
- ✓ Password established by the victim is entered into file



If subject does not appear to be the identity theft victim, the inquiring agency must confirm information prior to taking action

Notes:

When a person becomes aware that his/her identity has been stolen and reports the incident to law enforcement, the agency handling the identity theft case should create a victim profile in the Identity Theft File. The profile should include information such as the victim's name, date of birth, social security number, and type of identity theft.

In addition, a password is established by the victim and entered into the Identity Theft File. The password will only be known by the victim and he/she should be able to provide the password to law enforcement if they are the subject of the Identity Theft File. This password should not be shared with anyone; the victim should be able to provide the password when asked by the law enforcement agency that made the query on the file.

When an agency receives a record response to an NCIC query containing identity theft information and the person inquired upon does NOT appear to be identical with the subject of the Identity Theft File and/or does NOT know the assigned password, the inquiring agency must confirm the information prior to taking action based on the record information. This can be done by calling or sending a FAM to the entering agency.

1.49 Violent Person File

Violent Person File

A status record alerting agencies that an individual they are encountering may have the propensity for violence against law enforcement/ and or the public

- VPC1 - Assault on Law Enforcement
- VPC2 - Violent Crime Homicide/Attempted Homicide
- VPC3 - Violent Crime with Weapon
- VPC4 - Threat to Law Enforcement
- VPC5 - Threat of Targeted Violence

Notes:

The Violent Person File (VPF) contains status records that are designed to alert law enforcement officers that an individual they are encountering may have the propensity for violence against law enforcement, or poses a threat of targeted violence. All VPF records are considered law enforcement sensitive and should not be disseminated to the public or disclosed to the identified person of record. VPF records do not require hit confirmation.

The VPF can be classified under the following Violent Person Criteria (VPC):

VPC 1: Assault on Law Enforcement: 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.

VPC 2: Violent Crime Homicide/Attempted Homicide: Offender has been convicted of a violent offense against a person to include homicide and attempted homicide.

VPC 3: Violent Crime with Weapon: Offender has been convicted of a violent offense against a person where a firearm or weapon was used.

VPC 4: Threat to Law Enforcement: A law enforcement agency, based on its official investigative 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 community.

VPC 5: Threat of Targeted Violence: Agencies that maintain an established Behavioral Threat and Management (BTAM) process or program, may enter an identified person of concern who poses a threat of targeted violence. Entries are based upon documented information or evidence that predicates the threat of reasonably anticipated criminal conduct. This selection marks the record as an FCIC-only file.

1.50 Violent Person File

Violent Person File

Behavioral Threat Assessment and Management (BTAM) is a strategy used to mitigate or prevent targeted violence, regardless of motive, target, or social domain

- ✓ Entry is considered active criminal intelligence information
- ✓ Subject to 28 CFR Part 23 and may qualify for public record exemption
- ✓ File entry must be predicated upon reliable and valid information
- ✓ Instructional caveat advises of investigative coordination

For more information on the Violent Person File refer to CJIS Memos 2016-21 and 2021-13 located on the CJNet under CJIS Resources.

Notes:

BTAM entries of identified persons of concern for targeted violence is considered “active criminal intelligence information,” which is subject to 28 Code of Federal Regulation (CFR) Part 23 restrictions and may qualify for Florida public records exemption. File entry must be predicated upon reliable and valid information or evidence that establishes a reasonable suspicion of anticipated criminal conduct, and is contained within the entering agencies official investigative files or records.

An instructional caveat is provided immediately above a matching FCIC BTAM record, which advises users to ensure investigative coordination by contacting the entering agency to obtain additional information, or to report any observed or documented behavior(s) that may appear unusual, inappropriate, concerning, or threatening.

For more information on the Violent Person File refer to CJIS Memos 2016-21 and 2021-13 located on the CJNet under CJIS Resources.

1.51 Hit Confirmations

Hit Confirmations

A Hit is a 'positive response' received when a user queries a record in FCIC/NCIC


Hit alone is not probable cause to make an arrest, recover a missing person or seize property

Hit confirmation time limits

- Urgent = 10 minute response
- Routine = 1 hour response

Request Number Field:
2nd request sends notice to FDLE CSC
3rd request sends notice to FDLE CSC and FBI CJIS

The Hit confirmation process must be completed prior to taking action



Notes:

A hit is a “positive response” received when a user queries person or property records from FCIC and NCIC. A hit alone is not probable cause to make an arrest, however, a confirmed or verified hit may be adequate grounds to arrest a person, recover a missing person, or recover stolen property depending on the circumstances.

Hit Confirmation time limits are set according to the level of priority assigned by the requesting agency. Urgent hit confirmation requests require a ten-minute response, while Routine hit confirmation requests must be responded to within one hour.

The Request Number Field on the Hit Confirmation Request form, indicates the number of times the Hit Confirmation Request was sent. The first Hit Confirmation Request is selected when the operator sends the first request to the entering agency. The second request is selected when the entering agency has not responded to the first request. This second request not only goes to the entering agency, but also to the FDLE Customer Support Center (CSC). The CSC will contact the entering agency to inquire why the agency has not responded to the Hit Confirmation Request. The third request is selected when the entering agency has not responded to the second request. This third request will go to the entering agency and CSC again, and will also go to the FBI CJIS division for documentation.

Before an agency can take any official action on a Hot File record hit, the Hit

Confirmation process must be completed, including receiving a Hit Confirmation Response from the entering agency. The recovering agency should not place a locate or recover a person or property unless a Hit Confirmation Response has been received.

1.52 Locate

Locate

A Locate indicates that the person or property has been located and/or recovered

An agency that entered the record may not place a Locate

Exception – entering agency can place Locate on Wanted Person record if placing a Detainer

MIKE/WANTED PERSON
EXLT1- FULL EXTRADITION UNLESS OTHERWISE NOTED IN THE MIS FIELD
ORUFL030002 NAMTEST, TED SEXM RACW POB NY
DOB19800422HOT502 WGT135 EYE BLU HAIBLK
SM1TAT FLB00Y
SOC123456789
OFF BURGLARY- CPCL5
DOW20080428 OCAQAVE043002
WNO7DCH835A
DNAIN
ORI IS LEON COUNTY SO 850-573-8890
NCW000173214DTE20080430 1457 EDT DLU20080430 1457 EDT
IMMED CONFIRM WARRANT AND EXTRADITION WITH ORI

WARNING- A LOCATE HAS BEEN PLACED ON THE SUBJECT OF THIS RECORD.
PLEASE CONTACT ORI TO OBTAIN ADDITIONAL INFORMATION

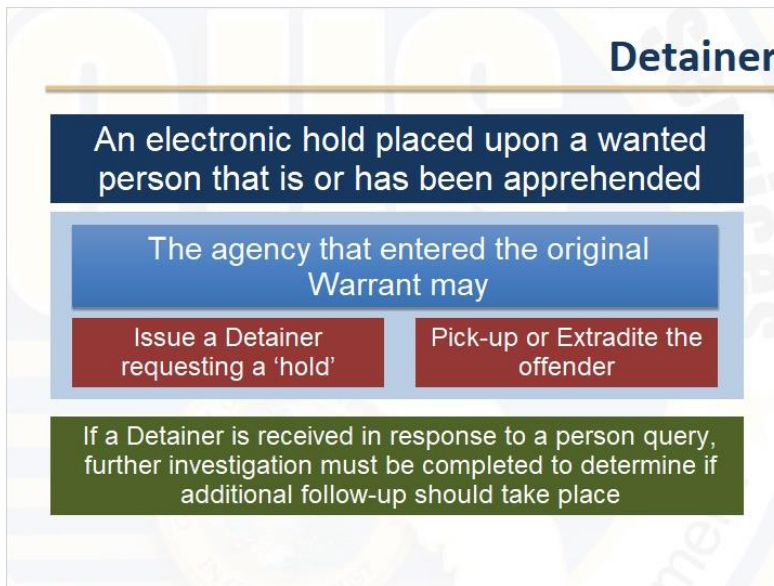
MIKE/LOCATED WANTED PERSON
EXLT1- FULL EXTRADITION UNLESS OTHERWISE NOTED IN THE MIS FIELD
ORUFL0370000 NAMTEST, TED SEXM RACW POB NY
DOB19800422HOT502 WGT135 EYE BLU HAIBLK CTZUS
SHN LGT
SOC123456789
OFF BURGLARY
DOW20100408 OCATEST-0409102
DNAIN
ORI IS ORANGE COUNTY SHERIFF'S OFFICE 407-239-4222
LOCATED20110408 FL0070500 TTT000
DOO20110408 ONOTEST11 RIUFL0070000
NCW0430000364DTE20100408 1519 EDT DLU20110807 1117 EDT
IMMED CONFIRM WARRANT AND EXTRADITION WITH ORI

Notes:

What is a Locate? An agency that recovers an FCIC/NCIC entry must place a Locate on the active record after a positive Hit Confirmation Response has been received from the agency of record. When this process has been completed, the record status will change. For example, a Wanted Person record will change to a LOCATED Wanted Person record. Some Limited Access operators have the capability to place Locates depending on the configuration of their FCIC/NCIC terminal settings.

Only the recovering agency can place a Locate on a hot file record, however, there is one exception to this rule. An entering agency may place a Locate on their Wanted Person record entry if the recovering agency is unable to place a Locate and the entering agency would like to place a Detainer on the Wanted Person. This is the only circumstance when the entering agency may place a Locate on their own record entry.

1.53 Detainer



Notes:

A detainer is an electronic hold on a person that has been apprehended and is being held at a correctional facility. The agency that entered the warrant may enter a detainer requesting that the person be held until the arresting agency's charges are satisfied. Once local charges are satisfied, the entering agency can then pickup/extradite the offender for the charges which initiated the warrant. While a Limited Access Operator cannot place a detainer, if a detainer is received in response to a person query in FCIC/NCIC, further investigation must be completed to determine if additional follow-up should take place.

1.54 Imagine this...

Imagine This...



Notes:

Imagine this, you are a new dispatcher at a local police department and receive a call from a detective with your agency. Detective Smith is requesting a wants and warrants check on a suspect he is investigating in reference to a sexual assault case. You query the subject's name and identifiers in FCIC and NCIC and receive quite a few responses. Included in the responses are a sex offender status flag, a protection order and a probation and parole record. Additionally, there are warrants for violation of probation and failure to register as a sex offender. As you are looking through these responses, you notice that some of the names and other identifiers don't match the person you queried. At this point, you are confused and not sure what to report back to Detective Smith. You ask another dispatcher. "Hey John, I just ran a check on a suspect in a sexual assault case for Detective Smith and got a lot of responses back. Some of the identifiers in the responses don't match the person I queried, so I'm not quite sure what to report to the detective."

1.55 Imagine this scenario continued...

<p>WARNING - DO NOT ARREST BASED ON THIS INFORMATION</p> <p>MIKE/SEXUAL OFFENDER ORIFL0370100 NAM/TEST,VINNY SEX/M RAC/W DOB/19600101 HGT/600 WGT/180 EYE/GRN HAIR/B0 FB/777777 SOC/123456789</p> <p>ORD/20060201 EDX/NONEXP SEX/WR CRISSEX OFFENSE - AGGRAVST CHILD FONDLING CON/20060201 OCA/20062 DNA/N SNU/9999 SNA/MAIN CTY/TALLAHASSEE STA/FL ZPR/00000 ORI IS FILE HDQ TALLAHASSEE B04 674 2038 NIC/X073033487 DTE/20060329 1228 EST DLU/20190329 1228 EST</p> <p>MIKE/PROTECTION ORDER ORICA0249400 NAM/TEST,VINNY SEX/M RAC/W DOB/19600101 SOC/123456789 PNO/09876 BRD/U ISD/19990104 DXP/NONEXP FB/777777 PCO001 - THE SUBJECT IS RESTRAINED FROM ASSAULTING, THREATENING, ABUSING, PCO04ASSAULTING, FOLLOWING, INTERFERING, OR STALKING THE PROTECTED PERSON AND/OR PCO0THE CHILD OF THE PROTECTED PERSON. OCA/1234 DNA/N ORI IS BUR OF CRIMINAL ID & INFORMATION SACRAMENTO 916 227 3275 PCO005 - THE SUBJECT IS RESTRAINED FROM MAKING ANY COMMUNICATION WITH THE PCO0PROTECTED PERSON INCLUDING BUT NOT LIMITED TO, PERSONAL, WRITTEN, OR PCO0TELEPHONE CONTACT, OR THEIR EMPLOYERS, EMPLOYEES OR FELLOW WORKERS NIC/H059037840 DTE/20050517 1308 EDT DLU/20190517 1308 EDT</p>	<p>WARNING - DO NOT ARREST BASED ON THIS INFORMATION</p> <p>MIKE/PROBATION OR SUPERVISED RELEASE STATUS ORIFL0370142 NAM/TEST,TEST SEX/M RAC/W DOB/19600101 HGT/600 WGT/200 HAIR/BLK QLN/000000000 OLS/FL OLY/2012</p> <p>OCA/111111111 MIS/1 DPE/20140101 DSS/20120101 EDS/20130101 SON/TEST,TEST SOT/050 555-5555 DNA/N ORI IS FL DEPT OF LAW ENFORCEMENT COMMAND CENTER 550 410-7000 NIC/C370106097 DTE/20110223 1415 EST DLU/20190223 1422 EST REPEAT - PROBATION OR SUPERVISED RELEASE STATUS RECORD - DO NOT ARREST BASED ON THIS INFORMATION - PLEASE CONTACT SUPERVISING AGENCY VIA NLETS, TELEPHONE OR EMAIL TO ADVISE OF CONTACT WITH SUPERVISED INDIVIDUAL.</p> <p>MIKE/WANTED PERSON EXL/1 - FULL EXTRADITION UNLESS OTHERWISE NOTED IN THE MIS FIELD ORI/NY001015Y NAM/TEST,VINNY SEX/M RAC/W DOB/19600215 HGT/600 WGT/200 HAIR/BLK SOC/111111111 OFF/ SEX OFFENSE DOW/20061124 OCA/OATSTN08 MIS/BEE VOR FAILURE TO REGISTER AS A SEX OFFENDER VIN/80464445456453454077 VYR/1999 VMA/CHEV VMO/C35 VST/PK VCO/GRY DNA/N ORI IS NY STATE DIV CRIMINAL JUSTICE SVCS ALBANY 510 457-6061 NIC/W410010455 DTE/20061124 1022 EST DLU/20191124 1022 EST IMMED CONFIRM WARRANT AND EXTRADITION WITH ORI</p>
---	---

Notes:

“Let me take a look...Well..... It looks like this guy has a protection order against him but I'm not sure about these other responses. You should go ask Sgt. Jones. He's our FAC.”

“I'll check with him.” “Sgt. Jones, I just ran a warrants check on a suspect in a sexual assault case for Detective Smith and got these responses back. Can you take a look?”

“Well.....it appears that this subject has a protection order against him and is also a registered sex offender. If you look closely, sometimes the name matches in the responses but the dates of birth and social security numbers don't. Just make sure you look through all the responses thoroughly to make sure the hit matches the person you queried.”

“Thanks, that helps a lot. I'll report this to Detective Smith”.

1.56 FCIC Agency Coordinator



Notes:

The FCIC Agency Coordinator, or FAC, serves as an agency's point of contact, both internally and externally, in matters regarding FCIC/NCIC. The FAC also serves as the liaison between the local agency and FDLE in CJIS matters. The FAC is responsible for ensuring that their agency is in compliance with applicable state and national policies governing the use of FCIC, NCIC, and Nlets systems.

1.57 FCIC Agency Coordinator

FCIC Agency Coordinator

To identify who serves as your agency FAC

Ask Supervisor

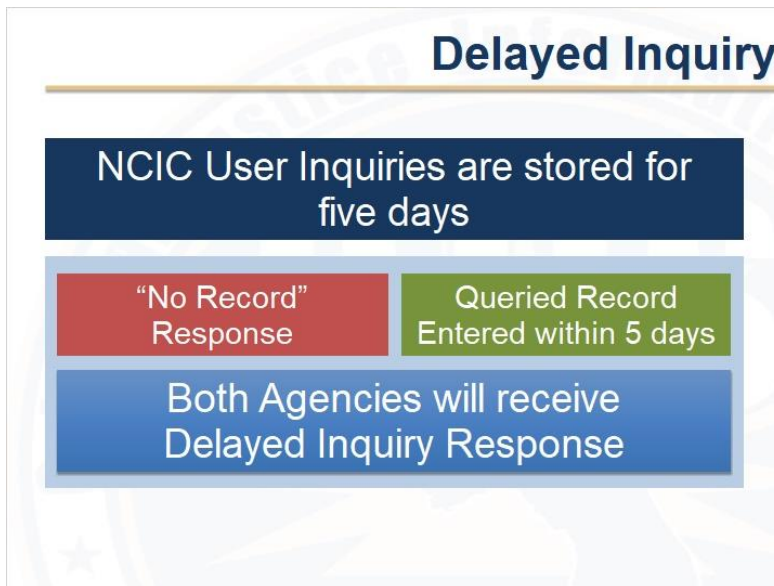
Contact
FDLE Customer
Support Center
(800) 292-3242



Notes:

Do you know who serves as the FAC and Alternate FAC for your agency? If you don't know, you can ask your supervisor or call the FDLE Customer Support Center at (800) 292-3242.

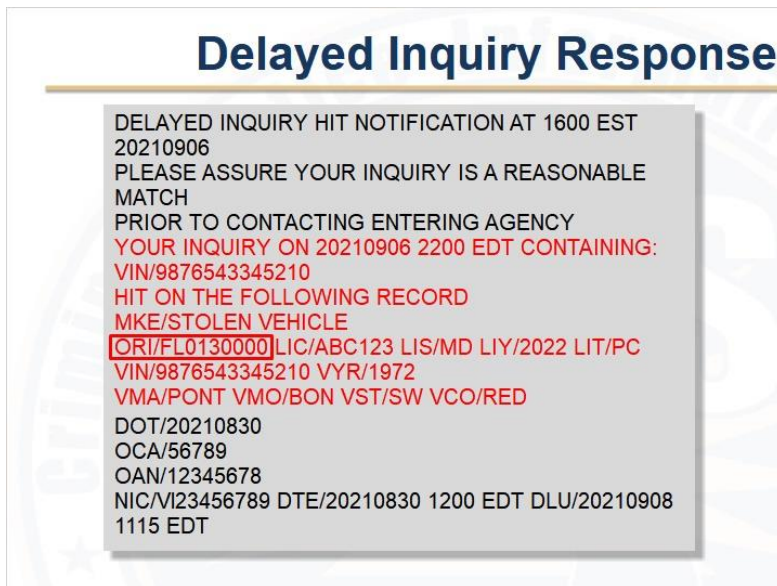
1.58 Delayed Inquiry



Notes:

NCIC user queries are stored for five days. If a user conducts a query and receives a “no record” response result, but within five days another agency enters a record containing information that matches the original query, both agencies will receive a Delayed Inquiry Response alerting them of each other's record entry or query. For example, a query made during a roadside stop on a vehicle prior to it being entered as stolen would trigger a notification to both the entering and querying agencies after the entry is made.

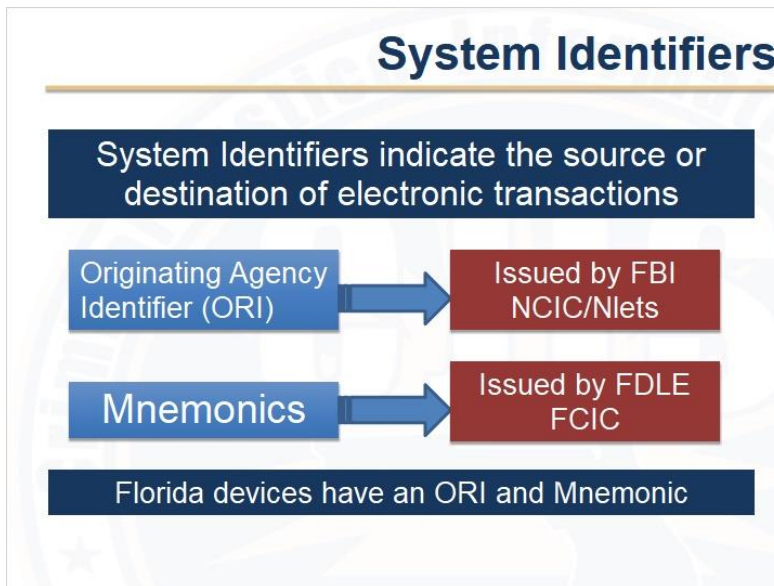
1.59 Delayed Inquiry Response



Notes:

This is an example of a delayed inquiry notification for a stolen vehicle. Notice that the delayed inquiry hit notification provides the inquiry date and Vehicle Identification Number, or VIN, for the vehicle that was queried. It also provides the vehicle information that was received as the hit or match; including VIN, tag number and state, as well as the make, model and color of the vehicle. The ORI of the entering agency is available if the querying agency would like to contact the entering agency.

1.60 System Identifiers

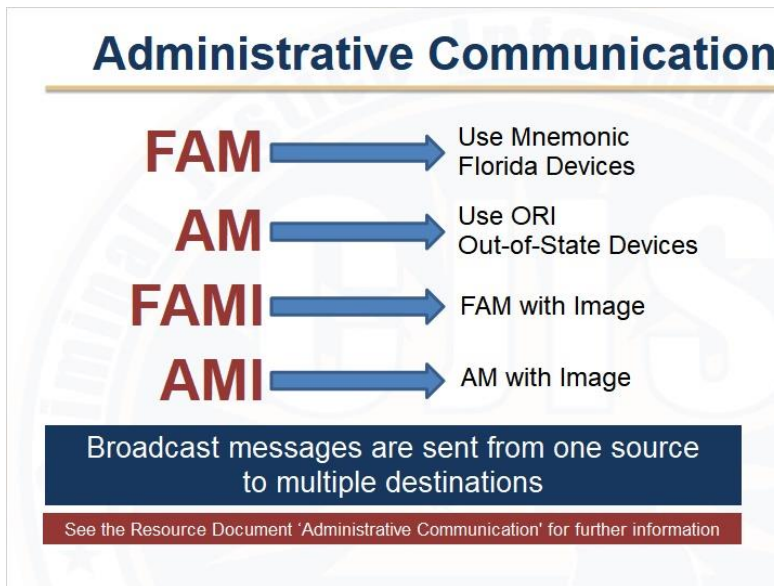


Notes:

FCIC, NCIC and Nlets use system identifiers to indicate the source or destination of electronic transactions. The FBI assigns Originating Agency Identifiers, or ORIs. Each agency is issued a primary ORI, and devices or groups of devices within the agency are also assigned ORIs. These alphanumeric identifiers are used to identify the agency during NCIC and Nlets transactions, as well as hit confirmations.

FDLE assigns mnemonics to each device in the state of Florida that accesses FCIC. Mnemonics are used to identify the agency and specific device submitting or receiving an FCIC transaction. Every FCIC and NCIC device in the state of Florida will have both an ORI and mnemonic assigned.

1.61 Administrative Communication



Notes:

Administrative communications are FCIC and NCIC free text messages. There are two message keys used for administrative communication: A Florida Administrative Message, or FAM, uses mnemonics to identify the source and destination of a message, and should be used when the sender and recipient are both within the state of Florida.

An Administrative Message, or AM, uses ORIs to identify the source and destination of a message, and should be used when either the sender or the recipient is outside of the state of Florida.

Images may be attached to administrative communication messages. The FAM with image, FAMI message key, allows the entry of an image with a FAM. The AM with image, AMI message key, allows the entry of an image with an AM.

A broadcast message may be used to send a message to multiple destinations at once. This includes groups of devices in Florida or groups of devices in multiple states. A BOLO is an example of a broadcast message. See the resource document 'Administrative Communication' for further information.

1.62 Guidelines for Communication



The graphic is titled "Guidelines for Communication" in a bold, dark blue font. Below the title is a large red rectangle containing the word "NO" in white, bold, sans-serif capital letters. To the right of "NO" is a dark red rectangle containing a bulleted list of prohibited items: "10 codes or signal codes", "Personal messages or holiday greetings", "Job or retirement announcements", and "Press releases". Below the red rectangle are two green rectangles. The first green rectangle contains the text "Include a signature which clearly identifies the agency and operator". The second green rectangle contains the text "Respond to messages in a timely manner".

Guidelines for Communication

- 10 codes or signal codes
- Personal messages or holiday greetings
- Job or retirement announcements
- Press releases

Include a signature which clearly identifies the agency and operator

Respond to messages in a timely manner

Notes:

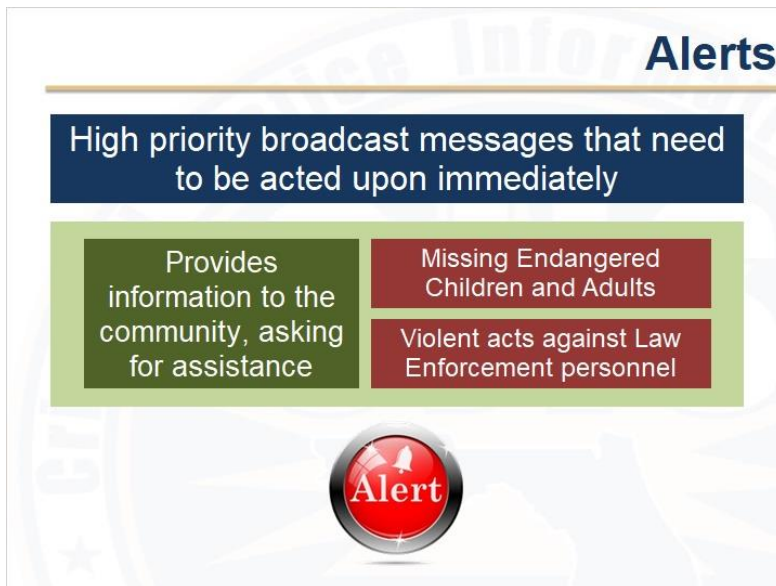
Users must follow basic guidelines when sending an administrative communication. These guidelines include using plain English, not using 10 codes or signal codes, not sending non-law enforcement related information such as personal messages, holiday greetings, job or retirement notices, and press releases.

Users sending administrative communication must also include a signature at the end of the message which clearly identifies the requesting agency, operator, and contact information. Additionally, if a user receives a request via administrative communication, they must respond within a timely manner.

Before sending a FAM or AM to the state control terminal for dissemination, take a moment to check for spelling errors which could impact the effectiveness of the message.

Agencies may receive communication via System Status Administrative Messages, often referred to as Dollar Sign Messages (\$). These messages can impact entries, modifications, locates, cancels or clears of FCIC/NCIC records.

1.63 Alerts Introduction




Notes:

There are certain special types of messages or Alerts that users should pay particular attention to. These are high priority notifications that need to be acted upon immediately. These alerts provide information to the community asking for assistance in the recovery of missing, endangered children or adults. Additionally, they provide information on violent acts against law enforcement personnel.


1.64 Alert Types

Alert Types



AMBER Alerts - High priority message issued when a child has been abducted and is endangered

Missing Child Alerts - Issued for a child who is missing and believed to be in danger, but doesn't meet the criteria for an AMBER Alert



When there is an immediate need for a child alert to be issued statewide, or within a geographical area, an Enhanced Missing Child Alert is utilized to alert the public that a child is in imminent danger due to the circumstances of their disappearance, autism, or other physical or mental disabilities.

Notes:

These message alerts include AMBER Alerts which contain critical, high priority information about child abduction cases. Missing Child Alerts refer to a child who is missing and believed to be in danger when there is no apparent sign of abduction, or does not meet all of the AMBER Alert criteria.

When there is an immediate need for a child alert to be issued statewide, or within a geographical area, an Enhanced Missing Child Alert is utilized to alert the public that a child is in imminent danger due to the circumstances of their disappearance, autism, or other physical or mental disabilities.

1.65 Alert Types

Alert Types



Silver Alerts - Issued for an adult who has experienced irreversible deterioration of mental capacity and is missing.

- For State Silver Alert: Person must be in an identified vehicle
 - FDLE assists with the FCIC Broadcast Message, media, public and roadside message alerts
- For Local Silver Alert: Person must be on foot
 - Local agency is responsible for FCIC Broadcast Message, media and public alerts

Notes:

Silver Alerts include subject and/or vehicle data about persons of a certain age who have experienced a deterioration of mental capacity (including dementia or Alzheimer's issues) and are lost or missing. A Silver Alert may be entered as a State or Local Alert.

For a State alert, the missing person must be in a vehicle. FDLE will assist the reporting agency by issuing the FCIC Broadcast Message, contacting the Media, and issuing public and roadside message alerts.

For a local alert, the missing person must be on foot. The local law enforcement agency is responsible for issuing the FCIC Broadcast Message by sending a FAM with subject code 34 "Silver Alert Activation". The local agency is also responsible for notifying the media and public of the missing person. Once the missing person has been recovered, the agency must cancel the local alert by sending a FAM using subject code 35 "Silver Alert Cancel".

1.66 Alert Types

Alert Types



Purple Alerts - Messages sent through FCIC that contain information about missing adults suffering from a mental or cognitive disability that is not Alzheimer's disease or a dementia-related disorder.

The Purple Alert must be disseminated to the geographic areas where the missing adult could reasonably be.


Notes:

The Florida Purple Alert is used to locate missing adults suffering from a mental or cognitive disability that is not Alzheimer's disease or a dementia-related disorder. Purple Alerts include a developmental or intellectual disability; a brain injury; other physical, mental or emotional disabilities that are not related to substance abuse; or a combination of any of these.

The Purple Alert must be disseminated to the geographic areas where the missing adult could reasonably be, considering his/her circumstances and physical and mental condition, the potential modes of transportation available, and the known or suspected circumstances of his/her disappearance.

1.67 Alert Types

Alert Types



Blue Alerts - These are messages sent through FCIC that contain information about law enforcement officers who have been killed, seriously injured, or are missing while in the line of duty and the suspect, who is considered to pose an imminent threat to the public, is still at large.

Each Alert message received should be immediately evaluated and forwarded to other pertinent members within the agency.

See the Resource Document 'Alerts' for further information about Alerts

Notes:

Blue Alerts include information regarding law enforcement officers who have been killed, seriously injured, or are missing while in the line of duty and the suspect, who is considered to pose an imminent threat to the public, is still at large. In Florida, Blue Alerts are sent out by FDLE's Intelligence Watch and Warning Section. See the resource document "Alerts" for further information regarding the activation of Amber, Missing Child, Silver and Blue Alerts.

1.68 Concealed Weapon Permit

Concealed Weapon Permit

Searchable by FL permit/ license number or
SSN if provided by permit holder

**CONCEALED WEAPON OR FIREARM LICENSE
STATE OF FLORIDA**

SAMPLE

DOE JOHN E.
23 SAMPLEVILLE AVENUE
ROSE DAIRY FL 00000

BIRTH DATE	SEX	RACE
00/00/00	M	B

LICENSE NUMBER	ISSUED	EXPIRES
W 0000000	00/00/00	00/00/07

The above named individual is licensed by the Department of State, Division of Licensing in accordance with Section 790.06, Florida Statutes.

Katherine Harris
KATHERINE HARRIS
SECRETARY OF STATE

Notes:

Concealed Weapon Permits issued by the state of Florida may be searched in FCIC by either a Concealed Weapon Permit/license number or by social security number (SSN). Per Florida Statute the SSN field is optional for Concealed Weapon Permit applicants. Please be advised that a query by SSN will only return results if the permit holder opted to provide this information at the time of application. An SSN search may not be conclusive, and negative results may require further investigation by contacting the Florida Department of Agriculture and Consumer Services. Responses are only provided on current Florida licenses and those that have expired within the last two years. Finally, the Concealed Weapon Permit search is restricted only to users at a law enforcement agency in connection with the performance of lawful duties.

1.69 Concealed Weapon Permit

Concealed Weapon Permit

Certain states provide automated responses to Concealed Weapon Permit queries



Refer to www.nlets.org for a current map of states that respond to the Concealed Weapon Permit Query.

Notes:

Nlets also allows for out-of-state Concealed Weapon Permit queries. Refer to www.nlets.org for a current map of states that respond to the out of state Concealed Weapon permit Query.

1.70 Investigative Tools

Investigative Tools


FDLE maintains a log of FCIC/NCIC queries and responses made on Florida devices for five years

TAR data can be used for:

- ✓ Criminal investigations
- ✓ Administrative purposes
- ✓ Misuse Investigations

Florida device logs are requested from FDLE
Out-of-state logs are requested from FBI CJIS

See the Resource Document 'Investigative Tools' for further information



Notes:

FDLE maintains a message log of all queries and responses made and received on Florida devices for five years. This FCIC and NCIC archived data, called a Transaction Archive Report, or TAR, can be used in criminal investigations, administrative purposes or misuse investigations. To obtain transaction log information for Florida device queries and responses, contact FDLE. For out-of-state transactions, or for archived information older than 5 years, contact the FBI.

Refer to the resource document “Investigative Tools” for further information.

1.71 Transaction Archive Report (TAR)

Transaction Archive Report

TAR requests must include:

- ✓ Your name and phone number
- ✓ Your agency name and ORI
- ✓ Specifics of request
- ✓ Time frame
- ✓ Reason for request

FDLE Transaction Archive Report (TAR)
2012-06-22 08:55:50

Search Parameters
Requestor: FDLE IDT
Request Date: 2012-06-22
Reason: Administrative
Range: 2012-06-21 00:00:00 to 2012-06-22 00:00:00
Free Text: (UNKNOWN USER)
Elapsed Time: 00:01:53 (Status: Done, 40 of 40 hits printed.)

Messages
2012-06-21 12:26:00.483 66858893 QV S13004462 O
<HDR>: [UCD]: DEV: 00001 [MNE]: S13004462 [HIT]
[CTL]: 105874
[IAF]:
[DATE]: 20120621 [TIME]: 1226 [NBR]: 00520
<MIKE>: QV
<ORI>: FL01366M0
<LIC>: 832TJR
<LIS>: FL
--ERROR--
UNKNOWN USER CODE PLEASE NOTIFY TAC
--END--

Notes:

To request a Transaction Archive Report from FDLE, send an email to TARRequest@fdle.state.fl.us. In your email request, be sure to include your name, phone number, agency name and ORI, the specifics of your request, a time frame you believe the transaction occurred, and the reason for making the request. For misuse investigations also provide the device Mnemonic the transaction occurred on, or the user's name that you are inquiring about.

1.72 CJIS Security Policy

CJIS Security Policy

FDLE has adopted the FBI CJIS Security Policy

Agencies that do not meet the standards set forth by the CJIS Security Policy may receive a letter of non-compliance following a Records Compliance or Technical audit in addition to facing possible sanctions and disciplinary actions



Improper handling and sharing of CJI can result in criminal and/or civil prosecution

Notes:

FDLE has adopted the FBI's CJIS Security Policy as the foundation for all Criminal Justice related information security and adheres to the rules and regulations stated in the Policy. Agencies that are found to not meet these standards following a CJIS Records Compliance or Technical audit may receive a letter of non-compliance, possible sanctions and agency issued disciplinary actions. Improper handling and sharing of Criminal Justice Information is a violation of CJIS Security Policy, can result in criminal and/or civil prosecution, and could potentially expose a criminal justice agency to liability.

1.73 System Vulnerabilities and Threats


Vulnerabilities and Threats

Vulnerability - a condition or weakness that could be exploited by a threat

Threat - any circumstance or event with the potential to cause harm

Types of threats may include:

- ✓ Natural
- ✓ Unintentional
- ✓ Intentional



Notes:

One of the greatest threats to an agency's Information Technology (IT) system is from users within the agency. A vulnerability is a condition or weakness in a data system that could be exploited by a threat. A threat is any circumstance or event with the potential to cause harm.

Natural, Unintentional, and Intentional are different types of threats that can compromise IT systems. Natural threats include hurricanes, water, lightning, and heat. Unintentional threats might include a user who accidentally erases a critical file while “playing” on the computer. Other intentional threats include hackers and malware.

Through the implementation of the required IT security outlined in the CJIS Security Policy, all users can ensure the confidentiality, integrity, and availability of criminal justice data.

1.74 System Vulnerabilities and Threats

Vulnerabilities and Threats

Social engineering is an IT security threat

Social engineering can occur

- ✓ Over the phone or in person
- ✓ By shoulder surfing
- ✓ Via email
- ✓ Through text

The threat may be internal or external


Notes:

The most serious threats are intentional and include social engineering. Social engineering can be carried out over the phone or in person. An example includes someone phoning an agency claiming to be an official IT person that is working on the agency's IT system, or it can be as simple as shoulder surfing, someone looking over your shoulder to get your password. Social engineering can also be conducted by email or even by text. However it occurs, social engineering is a viable and real threat that can occur either internally or externally.

1.75 Access Security

Access Security

- ✓ Each agency shall implement the most restrictive set of rights or access needed by users
- ✓ Limits access of Criminal Justice Information to only authorized personnel
- ✓ Need and right to know
- ✓ Immediately removing access




Notes:

Each agency shall implement the most restrictive set of rights or access needed by users for the performance of specified tasks and/or duties necessary to reduce the risk to Criminal Justice Information. This limits access of Criminal Justice Information to only authorized personnel with the need and right to know. This includes immediately removing FCIC/NCIC access for personnel who leave the agency or changes to a position and no longer requires access.

1.76 User Accountability

User Accountability

- ✓ Users may only share Criminal Justice Information with authorized criminal justice/law enforcement personnel
- ✓ CHRI may only be disseminated to authorized recipients using secure devices
- ✓ Dissemination of CHRI must be completed in a secure manner
- ✓ Electronic dissemination of CHRI must meet encryption requirements if transmitted over a public network segment



Notes:

Users may only share Criminal Justice Information on a need to know, right to know basis with authorized criminal justice personnel. Dissemination of Criminal History Record Information (CHRI) to another agency is allowed only to authorized recipients using secure devices. Electronic dissemination of CHRI must also meet encryption requirements if transmitted over a public network segment. Things to think about: Does the other agency have a valid ORI? Have I completely logged my dissemination to that agency in a secondary dissemination log?

1.77 User Accountability

Use of Acknowledgement Statement

- Each user is accountable for the access and use of CJ
- Prior to accessing a CJ system, the user must confirm an acknowledgement statement which shall include the following:
 - The user is accessing a restricted information system
 - System usage may be monitored, recorded and subject to audit
 - Unauthorized use of the system is prohibited and may be subject to criminal and/or civil penalties
 - Use of the system indicates consent to monitoring and recording

Notes:

Each user is accountable for the access and use of Criminal Justice Information. Upon accessing a criminal justice system, a system use notification message is required to remind users that Criminal Justice Information is restricted information; system usage may be monitored, recorded and subject to audit; unauthorized use of the system is prohibited and may be subject to criminal and/or civil penalties; and the use of the system indicates the user consents to the monitoring and recording of their usage.

1.78 Handling of Criminal Justice Information (CJI)

Handling of CJI

Agencies and their users must ensure electronic media and printed documents that contain CJI, in transit or storage, are treated securely

- ✓ Electronic CJI data must be protected and encrypted
- ✓ Users should not copy and paste an FCIC/NCIC response
- ✓ Printed CJI data is disposed of by shredding or burning
- ✓ Electronic media used to store CJI must be physically destroyed or completely overwritten

Notes:

Agencies and their users must ensure electronic media and printed documents that contain criminal justice information, whether in transit or storage, are properly secured. Electronic Criminal Justice Information must be encrypted when outside an agency's CJIS Physically Secure Area. This includes criminal justice information stored on hard drives in laptops, scanners, copy machines, external hard drives, USB flash drives, digital memory cards, and other electronic media.

Before sending Criminal Justice Information over the Internet or any segment of a non-criminal justice-controlled network, including email and File Transfer Protocol (FTP) access to documents, the user must ensure the information is encrypted. Users should not copy and paste an FCIC/NCIC response into an email, record management or jail management system unless they have been notified by their FAC or Local Agency Security Officer (LASO) that the proper security is in place.

Printed Criminal Justice Information must be disposed of properly by either shredding or burning the documents. Electronic media used to store CJI must be physically destroyed or completely overwritten.

1.79 System Passwords


System Passwords

Password requirements defined in the FBI CJIS Security Policy include each user having

- ✓ A unique user name
- ✓ A strong password
- ✓ Practice secure password habits

Users shall

- ✓ Not share passwords or leave passwords in conspicuous locations
- ✓ Log off the software/system at the end of shift or when another user wants to use the software/system



Notes:

All computer software or systems accessing FCIC/NCIC, whether provided by FDLE, developed by a local agency or purchased from a vendor, must follow the password requirements defined in the CJIS Security Policy. Each user must have a unique user name, a strong password, and practice secure password habits.

Users shall not share passwords or leave passwords in conspicuous locations. Additionally, users shall log off at the end of their shift or when another user wants to access the computer system or software.

1.80 System Passwords

System Passwords

Minimum password requirements

- ✓ Shall be a minimum length of eight characters
- ✓ Shall not be a dictionary word or proper name
- ✓ Must include either one capitalized letter or number
- ✓ Passwords and the user ID shall not be the same

Agencies shall maintain systems

- ✓ Require passwords be changed within a maximum of every 90 days
- ✓ Prevent password reuse of the last ten passwords
- ✓ Not be transmitted in the clear outside the secure location
- ✓ Not displayed when entered

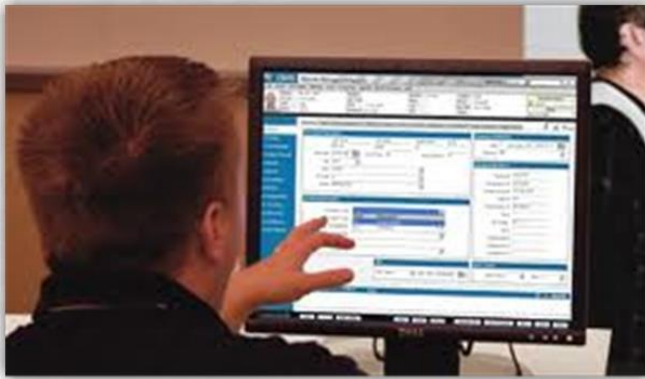
Notes:

The CJIS Security Policy sets the minimum password requirements for all users, as well as the password requirements for agencies that maintain systems that access Criminal Justice Information. Passwords shall be a minimum length of eight characters long; not be a dictionary word or proper name; must include either one capitalized letter or number; and passwords and usernames shall not be the same.

Additionally, agencies must maintain systems that access CJI and require password changes every 90 days, prevents the reuse of the last ten passwords, prevents the password from being transmitted over a public domain, and does not display the password when it is being entered.

1.81 Is this a violation of Security Policy?

A Violation of Security Policy?




Notes:

It is the graveyard shift at the intake desk of a jail. A supervisor, and an employee who just returned from vacation, are on duty. While the supervisor is on break, three deputies simultaneously bring in offenders to be booked, causing a backlog. The remaining intake employee attempts to login to FCIC/NCIC and discovers his Certification has inadvertently expired during his vacation, locking him out of the system. Feeling pressured by the deputies waiting, uncertain as to when the supervisor will return from break, and knowing that he will re-certify at the very first opportunity, the intake employee decides to use the login credentials of a fellow worker who keeps her password written down at her FCIC/NCIC workstation.

Is this a violation of the Security Policy? Yes. A user's login credentials are not to be shared, nor used, by other personnel. Additionally, users should not place their login credentials where other personnel can see them.

1.82 Physical Security

Physical Security



- ✓ Devices accessing FCIC/NCIC must be placed in a controlled area
- ✓ Authorized individuals are those who have a state and national background record check and training
- ✓ Strangers should be challenged and unusual activity reported
- ✓ Persons that make contact with an agency requesting protected information should be challenged
- ✓ Computers must have a 30 minute inactivity session lock

Notes:

Devices accessing FCIC/NCIC must be placed in an area controlled by a criminal justice agency where only agency authorized individuals have access to the screen, printer, keyboard and other storage devices. Authorized individuals include those that have had a state and national fingerprint-based background check, have completed the appropriate level of security awareness training or FCIC/NCIC Certification, and have been approved by the agency to have access to CJI. Strangers should be challenged and unusual activity should be reported to the agency's LASO or FAC. Persons that contact an agency requesting protected information such as how to access the network, the type of information that can be obtained electronically, etc., should be challenged. Personnel that are authorized to assist the agency with IT issues should not be asking a regular user about specific network or computer configurations.

Agencies and/or users must have a 30-minute inactivity session lock on computers accessing criminal justice information which requires a login to access the computer, such as a screen saver with a password. Vehicle Mobile Data Terminals (MDT) locked in the conveyance and dispatch computers located in a CJIS Physically Secure Location are exempt from this requirement.

1.83 Physical Security

Physical Security

- Access to areas that process CJI must be controlled to prevent unauthorized entry
- The agency must control access to devices that display FCIC/NCIC/CHRI
 - ✓ No devices may be placed in public spaces
- Visitors must be accompanied and monitored by authorized agency personnel at all times

Notes:

Agencies must control access to areas that process CJI to prevent unauthorized entry. Additionally, agencies must control access to the devices that display FCIC, NCIC and CHRI and may not place devices that access these systems in public areas. All visitors within CJIS Security Policy defined secure locations and areas where CJI is being processed, must be accompanied and monitored by authorized agency personnel at all times.

1.84 Network and Desktop Security

Network and Desktop Security

- ✓ Virus protection software installed and updated regularly
- ✓ Agencies shall implement spam, spyware protection and encryption
- ✓ Employ advanced authentication when accessing CJI outside of secure location
- ✓ Users should work with agency IT staff to minimize data loss



Notes:

All computers accessing FCIC/NCIC or the CJNet must have virus protection software installed and updated regularly. This software is used to protect the computer from Viruses, Worms, Trojan Horses and other malicious codes. Agencies shall implement spam and spyware protection, and encryption-controlled interfaces such as firewalls, gateways, and routers, to protect Criminal Justice Information. Additionally, agencies shall employ advanced authentication to systems when accessing CJI outside of a physically secure location.

Users should be cautious when opening email attachments from unknown senders. These attachments could contain viruses and other malicious codes intended to cause harm. Users should also work with agency IT staff to minimize data loss caused by inconsistent or poor power supplies.

1.85 Mobile and Wireless Security

Mobile and Wireless Security

- ✓ Prevent unauthorized access to mobile, remote and wireless devices
- ✓ Vulnerable to security threats
- ✓ All security features enabled
 - Cryptographic authentication = 128 bit encryption
 - Must meet Federal Information Processing Standards 140-2 (FIPS)
 - Firewall
 - Use authentication
 - Advanced Authentication (AA)
- ✓ Special reporting procedures for mobile devices include
 - Loss of device control
 - Total device loss or compromise in or out of the United States



Notes:

Each agency shall have written policies defining security practices to prevent unauthorized access to mobile, remote, and wireless devices. Handheld and wireless devices include Smartphones, Laptops, Tablets, and Air cards. These devices are especially vulnerable to security threats because of loss, theft or disposal, unauthorized access, electronic eavesdropping, electronic tracking, and cloning. Handheld and wireless devices shall have all of their security features enabled and special reporting procedures shall be in place. These procedures include loss of device control; total device loss or device compromise whether in or outside of the United States.

1.86 Non-Agency Issued Device Security

Non-Agency Issued Device Security



- ✓ Personally owned equipment and software shall not be authorized to access, process, store or transmit CJI
- ✓ Utilizing publicly accessible computers to access, process, store or transmit CJI is prohibited

Notes:

Personally owned equipment and computer software shall not be authorized to access, process, store, or transmit Criminal Justice Information. Utilizing publicly accessible computers such as those located at hotel business centers, convention centers, public libraries, and public kiosks to access, process, store, or transmit Criminal Justice Information is also prohibited.

1.87 Security Incident

Security Incident

A violation or possible violation of the technical aspects of the CJIS Security Policy

- ✓ Appearance of new files with strange names
- ✓ Mysterious new user accounts
- ✓ Accounting discrepancies
- ✓ Changes in file lengths or modification dates
- ✓ Data modification or deletion
- ✓ Denial of service
- ✓ Unexplained poor system performance
- ✓ Compromise of CJI including technical and physical loss of printed data
- ✓ Suspicious probes or browsing

Notes:

A security incident is a violation, or possible violation, of the CJIS Security Policy that threatens the confidentiality, integrity or availability of FCIC/NCIC. Some examples of security incidents include: the appearance of new files with strange names; mysterious new user accounts; accounting discrepancies; changes in file lengths or modification dates; data modification or deletion; denial of service; unexplained poor system performance; any compromise of CJI, including technical and physical loss of printed data, and suspicious probes or browsing.

1.88 Security Incident

Security Incident



- ✓ Follow agency's written policy describing actions to be taken during a security incident
- ✓ Report to the agency's Local Agency Security Officer (LASO) who will in turn forward a report to the FDLE CJIS Information Security Officer (ISO)

Notes:

Users may only see indicators of a security incident and shall follow their agency's written policy describing actions to be taken during an FCIC/NCIC or CJNet security incident. The operator shall take any precautions necessary to prevent unauthorized access to the network. This may include unplugging the network cable or air card, and/or disabling the wireless device. Any possible security incident should be reported to the agency's LASO who will in turn forward a report to the FDLE CJIS Information Security Officer.

1.89 Security Incident



Notes:

Think about this... You sit down at your terminal to log on to your computer. You notice that a new user account has been created and do not recognize the user name. What do you do? You should follow your agency's written policies.

1.90 Agency's Security Responsibility

Agency's Security Responsibility

The agency shall approve individual access privileges and shall enforce physical and logical access restrictions

The agency shall enforce the most restrictive set of rights/privileges or access needed by users

The agency shall implement least privilege access based on specific duties, operations or information systems as necessary to reduce risk to CJI

Ensure connections to the Internet, other external networks, or information systems occur through controlled interfaces

Notes:

The agency is responsible for the security of their IT system and how it connects to the state and national systems. The agency shall approve individual access privileges and shall enforce physical and logical access restrictions associated with changes to the information system. The agency shall enforce the most restrictive set of rights and privileges or access needed by users for the performance of specified tasks and accounts. Additionally, the agency shall implement least privilege access based on specific duties, operations or information systems as necessary to reduce the risk to CJI. Ensuring connections to the Internet, and other external networks or information systems, are made through controlled interfaces such as firewalls, gateways and routers is also required to ensure network and system security.

1.91 Misuse of Criminal Justice Information (CJI)

Misuse of CJIS Information and Systems

F.S. 112 sets forth the expectations of public employees behavior and ethics

Ethics is described as the rules and standards governing the conduct of a person and members of a profession

Users are expected to:

- ✓ Comply with policies and procedures relative to all CJIS systems
- ✓ Adhere to the highest standards of ethics and professional conduct

Notes:

Florida Statute 112 sets forth the expectations of public employees relative to the need and requirement for ethical behavior in all of their interactions. Ethics is described as the rules and standards governing the conduct of a person or the conduct of the members of a profession. Users are expected to comply with policies and procedures relative to all CJIS systems and adhere to the highest standards of ethics and professional conduct.

1.92 Misuse of Criminal Justice Information (CJI)

Criminal Justice Purposes

FCIC/NCIC are provided for official criminal justice purposes

The term "administration of criminal justice" is defined in F.S. 943.045(2) and 28 CFR Part 20.3, and includes

✓ Detection	✓ Rehabilitation of accused persons
✓ Adjudication	✓ Pre-trial release
✓ Apprehension	✓ Criminal identification activities
✓ Correctional Supervision	✓ Post-trial release
✓ Detention	✓ Prosecution

Users shall only use information derived from a CJIS system for official criminal justice purposes only

Users should be aware that improper handling of CJI, PII and CHRI information is a violation of policy and could result in criminal prosecution

Notes:

FCIC and NCIC are provided to criminal justice agencies, and statutorily defined agencies, for official criminal justice purposes. The term "administration of criminal justice" is defined in Florida Statute Section 943.045(2) and 28 Code of Federal Regulations, or CFR, Part 20.3. The administration of criminal justice includes the terms listed. Users shall only use information derived from a CJIS system, which includes any information from FCIC, NCIC, Nlets, and CJNet, for official criminal justice purposes.

There are policies and procedures that govern all agencies and personnel using CJIS systems provided by FDLE. Users should be aware that the improper handling of CJI, PII, and CHRI information is a violation of policy and could result in criminal prosecution. Additionally, information contained in any CJIS system from other state computer files shall only be used for criminal justice purposes as authorized by Florida Statute.

1.93 Misuse of Criminal Justice Information (CJI)

Misuse of CJI

- Any access of CJI systems and/or dissemination of information obtained for non-criminal justice purposes are considered a misuse of the system
- The user is responsible for all transactions while logged into any CJIS system
- CJI transactions, regardless of application, are automatically logged and audited
- Users shall only access CJI data for their agency's assigned criminal justice related duties

Notes:

Any access of CJI systems and/or dissemination of information obtained for non-criminal justice purposes are considered a misuse of the system. While logged into a CJIS system, the user is responsible for any access or use of CJI obtained. Additionally, all CJI transactions, regardless of the type of system or application being used, are recorded and logged and subject to audit. Users should access CJI data only for their agency assigned work-related duties.

1.94 Common Types of Misuse

Common Types of Misuse

Most misuse cases being investigated stem from one of the following categories

- ✓ Affairs of the heart
- ✓ Political motivation
- ✓ Monetary gain
- ✓ Idle curiosity
- ✓ Helping out a friend or family member



Notes:

Of the misuse cases investigated, most will stem from one of the following categories: affairs of the heart, political motivation, monetary gain, idle curiosity, and/or trying to help out a friend or family member.

1.95 Examples of Misuse

Examples of Misuse

Affairs of the Heart: A deputy queries his ex-wife's boyfriend to see if he has a criminal history	Helping out a friend or family member: A friend owns a rental property and asks you to query a potential tenant's criminal history
Monetary Gain: Querying Criminal Justice Information and selling it to the public	Political Motivation: An elected public official queries the wife of his opponent to get her criminal background to use it against him
Idle Curiosity: A dispatcher is watching TV and queries a tag in the Presidential motorcade	

Notes:

Examples of misuse include: Affairs of the heart - a deputy queries his ex-wife's boyfriend to see if he has a criminal history; Monetary gain - querying Criminal Justice Information and selling it to the public; Idle curiosity - a dispatcher is watching TV and queries the tag in a Presidential motorcade; Helping out a friend or family member - a friend owns a rental property and asks you to query a potential tenant's criminal history; or Political motivation - an elected public official queries the wife of his opponent to get her criminal background to use it against him.

1.96 Statutes Addressing Misuse of CJI

Statutes Addressing Misuse of CJI

F.S. 839.26 sets forth punishment up to a 1st degree misdemeanor for financially benefiting from information derived in an official capacity

F.S. 815 sets forth punishment up to a 1st degree felony for 'willfully, knowingly and without authorization' taking or disclosing data, or unlawfully accessing computer systems or networks

See the Resource Document 'Misuse' for further information

Notes:

The following are Florida Statutes which address the misuse of CJI. These statutes reference both ethical and criminal violations which could be grounds for disciplinary action or termination.

F.S. 839.26 sets forth punishment up to a 1st degree misdemeanor for financially benefiting from information derived in an official capacity.

F.S. 815 sets forth punishment up to a 1st degree felony for 'willfully, knowingly and without authorization' taking or disclosing data, or unlawfully accessing computer systems or networks.

For more information regarding these statutes, please print and retain the resource document "Misuse".

1.97 You are Ready to Test

To Complete Training

The modular portion of the training has finished.

Limited Access users may begin the Limited Access Certification test. Full Access users must complete the Full Access Online training prior to taking test.

To record completion, close the browser window.

Notes:

You have completed the modular portion of the Limited Access Certification Course. Limited Access users may begin the Limited Access Certification test. Full Access users must complete the Full Access Online Certification training within fourteen (14) days prior to taking the cumulative certification exam. To record completion of the training, please close the browser window.