

Limited Access Output

1.1 Introduction



Notes:

Welcome to the Limited Access Certification Course brought to you by the Florida Department of Law Enforcement's Criminal Justice Information Services. At the completion of this course you will be directed to the nexTEST application to complete the Limited Access Certification Test.

1.2 Limited Access User

Limited Access User

- Limited Access User - 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) systems
- Depends on:
 - Job function/assignment
 - Type of product used to access FCIC/NCIC
 - Terminal/device settings and restrictions
- Limited Access users are not able to make Hot File record entries

Previous Next

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 the type of queries or receive the responses described in this certification course can depend on: the job function/assignment within the agency the user is performing; 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 Section Overview



Notes:

The Limited Access Certification training is comprised of six sections.

-Section One will provide an overview of the Florida Crime Information Center (FCIC), the National Crime Information Center (NCIC), the International Justice and Public Safety Network (Nlets), the Criminal Justice Network (CJNet), information provided by the Department of Highway Safety and Motor Vehicles (DHSMV) through FCIC, and information regarding Audits and Compliance;

-Section Two will highlight Criminal Justice Information (CJI), Criminal History Record Information (CHRI), Purpose Codes, Attention Fields, and the use and purpose of the Secondary Dissemination Log;

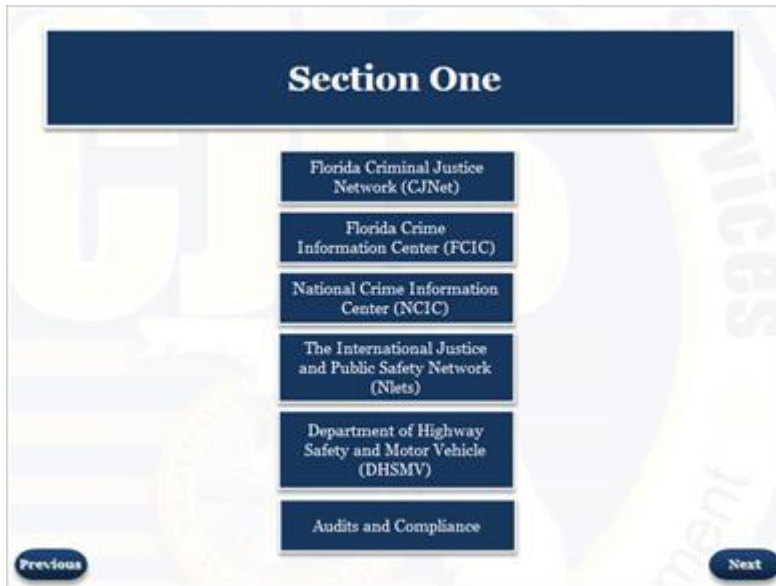
-Section Three will cover Hot Files, Locates and Detainers, Status Files and the duties of the agency's Terminal Agency Coordinator (TAC);

-Section Four will provide information on Unsolicited Messages, the various Alerts provided through the state and national systems, Concealed Weapon Permits and various Investigative Tools;

-Section Five will cover Security Awareness and;

-Section Six will provide important information on the repercussions of the Misuse of Criminal Justice Information (CJI).

1.4 Section One



Notes:

Section One contains six topics which include an overview of the various types of databases and information available within the Florida Criminal Justice Network or CJNet and the agencies that are allowed to access this information. The student will also learn about the various types of files and records available within FCIC, NCIC, and Nlets, and the departments that maintain and provide access to these databases. Information on the various FCIC records that are provided by the Florida Department and Highway Safety and Motor Vehicles through an FCIC query will be discussed. Lastly, the user will be introduced to the importance of CJIS Audit and Compliance.

1.5 The Florida Criminal Justice Network (CJNet)

The Florida Criminal Justice Network (CJNet)

- Provides access to state and national criminal justice resources relating to:
 - Law Enforcement
 - Judicial
 - Corrections
- Offers secure email services
- Access to criminal justice training calendar
- CJNet is provided only to Florida criminal justice and law enforcement agencies

Previous Next

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 secure email services for users 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.

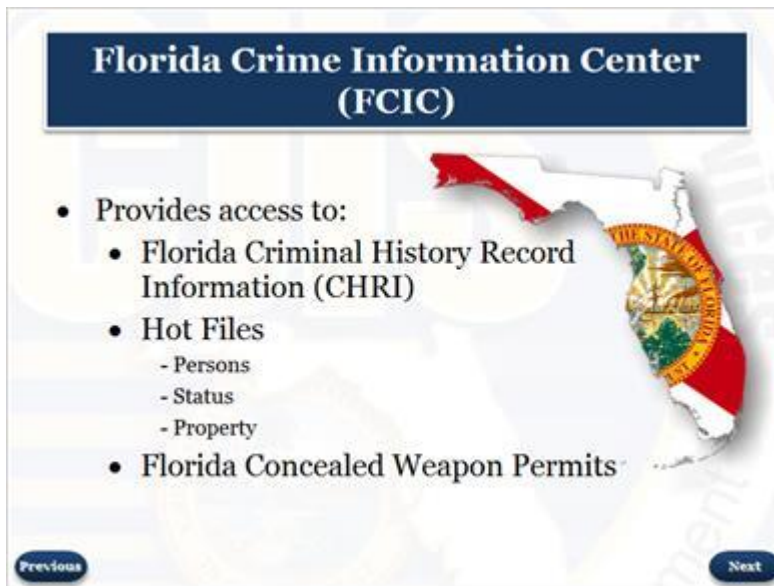
1.6 CJNet



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 frequent references such as Memorandums, Manuals, Regional Working Groups, 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.

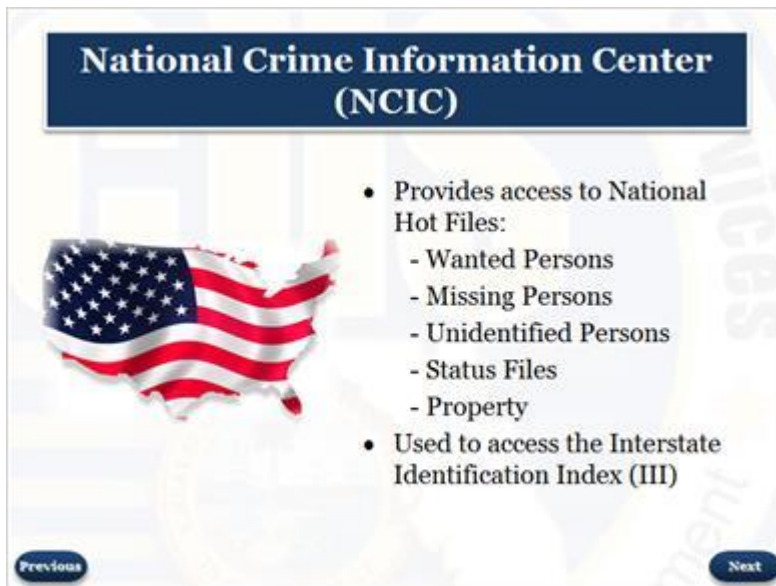
1.7 Florida Crime Information Center



Notes:

FCIC is the primary system used to access Florida records including Criminal History Record Information (CHRI), and Hot Files which includes Persons, Status, and Property records. 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.

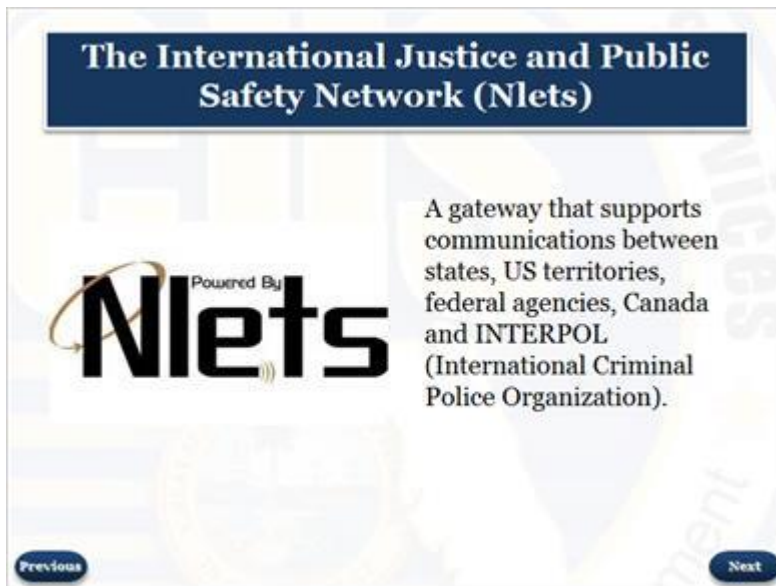
1.8 National Crime Information Center



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 US Virgin Islands, Guam, Canada, and all federal criminal justice agencies.

1.9 International Justice and Public Safety Network (Nlets)



Notes:

Nlets is a gateway that supports communication between states, US 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 computerized, 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 state databases.

1.10 International Justice and Public Safety Network (Nlets)

The International Justice and Public Safety Network (Nlets)

Common **out of state** Nlets transactions include the following:

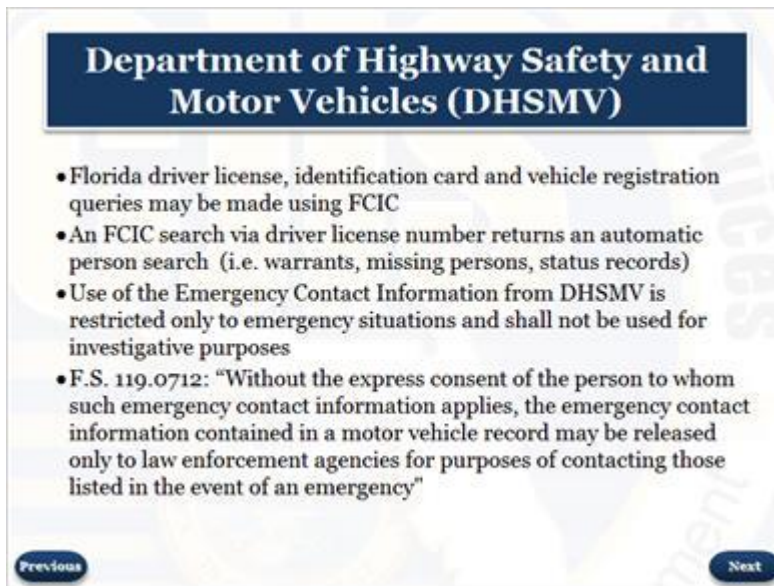
- Criminal history
- Vehicle registration
- Help files
- Concealed weapons
- Driver License
 - Running an out of state DL query may not return an automatic person query response

Previous Next

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. Please note that unlike a FCIC DL query response, which could include warrants, missing person or status records, when a user queries an out of state driver license through Nlets the user may not receive an automatic person response. For further information regarding Nlets transactions please visit the Nlets website at www.nlets.org.

1.11 Department of Highway Safety and Motor Vehicles (DHSMV)



The screenshot shows a presentation slide with a blue header bar containing the text 'Department of Highway Safety and Motor Vehicles (DHSMV)'. Below the header, there is a list of four bullet points. At the bottom of the slide, there are two buttons: 'Previous' on the left and 'Next' on the right. The background of the slide features a faint, large watermark of the word 'SAFETY'.

- Florida driver license, identification card and vehicle registration queries may be made using FCIC
- An FCIC search via driver license number returns an automatic person search (i.e. warrants, missing persons, status records)
- Use of the Emergency Contact Information from DHSMV is restricted only to emergency situations and shall not be used for investigative purposes
- 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:

Users may query DHSMV data through FCIC, and receive responses from DHSMV, FCIC, NCIC and perhaps Nlets, depending upon search criteria used. If a response is received via an FCIC query of a driver license number an automatic person search will occur that may include warrants, missing persons or status records. 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 (DHSMV)

When querying specified Florida specialty tags the user is required to enter additional "hidden" characters . Please print the attachment and maintain for your records.



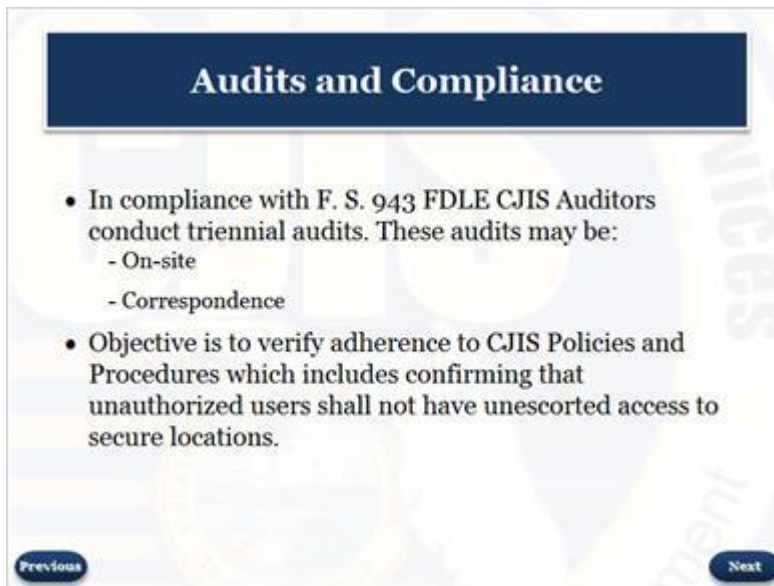
See the Resource entitled 'DHSMV - Specialized Tags' for further information to conduct searches on specialty tags.

[Previous](#)[Next](#)

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/digits that appear on the actual tag. Please refer to the resource entitled "DHSMV - Specialized Tags" for further information on how to query these "hidden" character tags. Please print this document and keep for future reference.

1.13 Audits and Compliance



Audits and Compliance

- In compliance with F. S. 943 FDLE CJIS Auditors conduct triennial audits. These audits may be:
 - On-site
 - Correspondence
- Objective is to verify adherence to CJIS Policies and Procedures which includes confirming that unauthorized users shall not have unescorted access to secure locations.

Previous Next

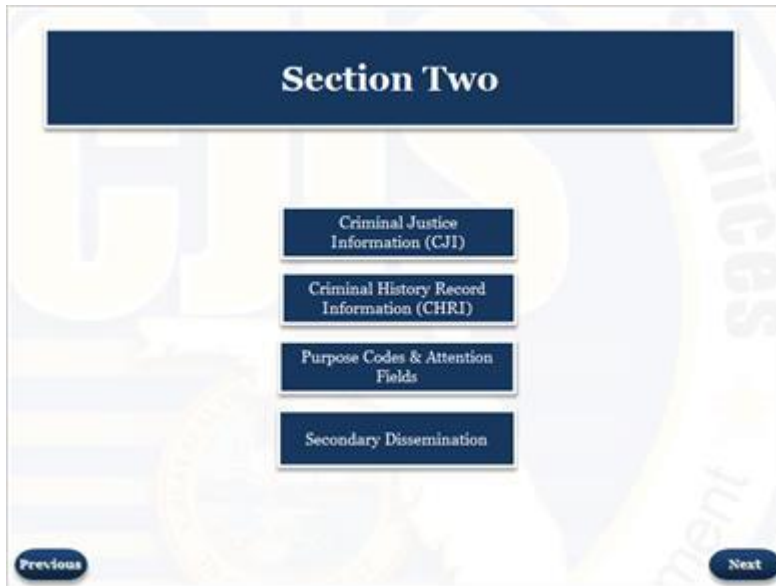
Notes:

In compliance with Florida Statute 943, FDLE CJIS Auditors will conduct either an on-site or mailed correspondence audit triennially on every criminal justice and law enforcement agency that has access to FCIC, NCIC and the CJNet.

The objective of the audit is to verify that the agency and agency users are adhering to the CJIS Policies and Procedures as well as the FBI CJIS Security Policy. Users should be aware that only authorized personnel can have unescorted access in areas that contain or have access to FCIC, NCIC, or the CJNet.

The information provided in this online Limited Access training includes policies and procedures you as a user must comply with in order for your agency to be in compliance during your agency's audit.

1.16 Section Two



Notes:

Section Two of the Limited Access Certification Course provides an overview of four topics. The first topic is Criminal Justice Information, or CJI, defining what it is and how it can be used. Next, guidance is provided on the use and access to CHRI, what it is used for and who is allowed to access CHRI. Purpose Codes and Attention Fields comprise the third topic along with the requirements for each when requesting CHRI. Finally, the definition of Secondary Dissemination of CHRI will be discussed and why a Secondary Dissemination log must be maintained.

1.17 Criminal Justice Information

Criminal Justice Information (CJI)

- Criminal Justice Information (CJI) refers to all of the FBI/FDLE CJIS provided data necessary for law enforcement and civil agencies to perform their missions, which include:
 - Biometric Data
 - Identity History Data
 - Biographic Data
 - Property Data
 - Case/Incident History

Previous Next

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 and civil agencies to perform their missions. 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.

1.18 Criminal History Record Information (CHRI)

Criminal History Record Information (CHRI)

- Sometimes referred to as "restricted data", and is considered a subset of CJI
- Shall be accessed only for an authorized purpose
- Dissemination of CHRI to another agency if:
 - The other agency is an Authorized Recipient
 - The other agency is performing personnel and appointment functions

Previous Next

Notes:

CHRI, sometimes referred to as "restricted data" is a subset of CJI. 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 and appointment functions for criminal justice employment applicants.

1.19 Personally Identifiable Information

Personally Identifiable Information (PII)

- Personally Identifiable Information (PII) is information used to distinguish or trace a person's identity such as:
 - 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

Previous Next

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.

1.20 Criminal History Record Information (CHRI)

Criminal History Record Information (CHRI)

CHRI can be obtained from the following:

- Florida Crime Information Center (FCIC)
 - Florida only
- National Crime Information Center (NCIC) Interstate Identification Index (III)
 - Multi-state and Federal
- International Justice and Public Safety Network (Nlets)
 - Direct access into other state repositories and Canada
- FDLE Fusion Center Watch Desk
- International Criminal Police Organization (INTERPOL)
 - Participating foreign countries, request made through state's INTERPOL liaison

Florida criminal history information is available to the public, for a fee, through FDLE's public website (www.fdle.state.fl.us) or by mail request.

[Previous](#) [Next](#)

Notes:

Criminal History Record Information or CHRI is available from multiple sources, and it may be necessary to make more than one inquiry to obtain an individual's complete criminal history. Criminal history inquiries 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 request CHRI directly from the state of record. An individual may also submit a request with the Florida Department of Law Enforcement's Fusion Center Watch Desk to acquire CHRI on persons from another country. The Fusion Center will contact the International Criminal Police Organization (INTERPOL) for assistance. Finally, the public may obtain Florida criminal history information, for a fee, by visiting www.fdle.state.fl.us.

1.21 Criminal History Record Information (CHRI)

Criminal History Record Information (CHRI)

- Used by law enforcement and criminal justice agencies for official purposes only
- Some non-criminal justice agencies are allowed access by Florida Statute (i.e. DCF, Public Defenders, etc.)
- 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

Previous Next

Notes:

CHRI should be used by law enforcement and criminal justice agencies for official criminal justice purposes only. Some non-criminal justice agencies are allowed access to CHRI by Florida statute or 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.

A common issue for agency non-compliance during a CJIS Audit is a user not understanding the information that is returned when running a criminal history or the functionality of the software used to retrieve criminal history information. 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.

1.22 Criminal History Record Information (CHRI)

Criminal History Record Information (CHRI)

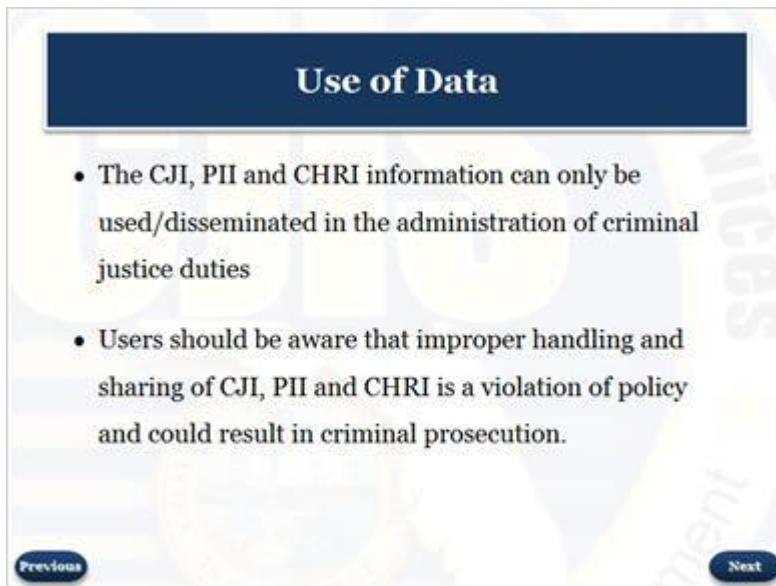
- Should not be kept in personnel files
- Are disseminated only as part of the user's criminal justice duties on a need to know, right to know basis
- Should not be shared with friends, relatives or the public
- May only be used for criminal justice purposes
- May be modified, updated or changed any time new information is received

Previous Next

Notes:

Additionally, 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. 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.

1.24 Use of Data



Use of Data

- The CJI, PII and CHRI information 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 is a violation of policy and could result in criminal prosecution.

Previous Next

Notes:

The CJI, PII and CHRI can only be used 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.

1.25 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 Livescan. Next, the fingerprints are electronically sent and compared by FDLE personnel against prints recorded 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 ID (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.

1.26 Florida Criminal History

Florida Criminal History									
--FLORIDA CCH RESPONSE--									
ATN/IDT-JR									
FC.DLE/01777559.PUR/C.ATN/IDT-JR									
SID NUMBER: 1777559 PURPOSE CODE:C PAGE: 1									
BECAUSE ADDITIONS OR DELETIONS MAY BE MADE AT ANY TIME,									
A NEW COPY SHOULD BE REQUESTED WHEN NEEDED FOR FUTURE USE									
- FLORIDA CRIMINAL HISTORY -									
NAME	STATE ID NO.	FBI NO.	DATE REQUESTED						
PUBLIC, CARL C	FL-01777559	9003300	03/06/2012						
SEX	RACE	BIRTH DATE	HEIGHT	WEIGHT	EYES	HAIR	BIRTH PLACE	SKIN	DOC NO.
M	W	05/23/1956	5'09"	153	HAZ	BLN	FL	FAR	
--CONTINUED--									
SID NUMBER: 1777559 PURPOSE CODE:C PAGE: 2									
FINGERPRINT CLASS	SOCIAL SECURITY NO.		MISCELLANEOUS NO.						
SCR/MRK/TAT									
CI PO 12 17 13			SC R ARM						
16 11 12 13 14									
OCCUPATION	ADDRESS		CITY/STATE						
CARPENTER	1110 N MONROE ST		TALLAHASSEE, FL						

Previous Next

Notes:

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.

1.27 Florida Criminal History

Florida Criminal History

ARREST - 1 06/12/1982 CBTS NO. -
-CONTINUED-
SID NUMBER: 1777559 PURPOSE CODE C PAGE: 3
ARREST AGENCY LEON COUNTY SHERIFF'S OFFICE (FL0370000)
AGENCY CASE: 1489 OFFENSE DATE: 06/12/1982
CHARGE 001-AGGRAV ASSLT-POL OFF-STDARM
BATTERY
STATUTE/ORDINANCE-FL784.06 LEVEL-FELONY
CHARGE 002-RESISTING OFFICER-
STATUTE/ORDINANCE-FL843.01 LEVEL-
JUDICIAL-
AGENCY LEON COUNTY SHERIFF'S OFFICE (FL0370000)
CHARGE 001-COURT SEQ COURT NO. -
COURT DATA-AGGRAV ASSLT-POL OFF-STDARM
BATTERY
-CONTINUED-
SID NUMBER: 1777559 PURPOSE CODE C PAGE: 4
STATUTE/ORDINANCE-FL784.06 LEVEL-FELONY
DISP DATE: 01/30/1982 DISP-CONVICTED
CONFINEMENT-000
CHARGE 002-COURT SEQ COURT NO. -
COURT DATA-RESISTING OFFICER-
STATUTE/ORDINANCE-FL843.01 LEVEL-
STATUTE DESCRIPTION-WITH VIOLENCE
DISP DATE: 01/30/1982 DISP-ADJUDICATION WITH/HEL
PROBATION-1Y

Previous Next

Notes:

CHRI elements include arrests, disposition, and sentencing information. Additionally information on criminal registrations, sexual predator and offender registrations, and clemency may also be included in the CHRI. For more information on reading and running criminal histories contact your TAC for information on available CJIS courses in your area.

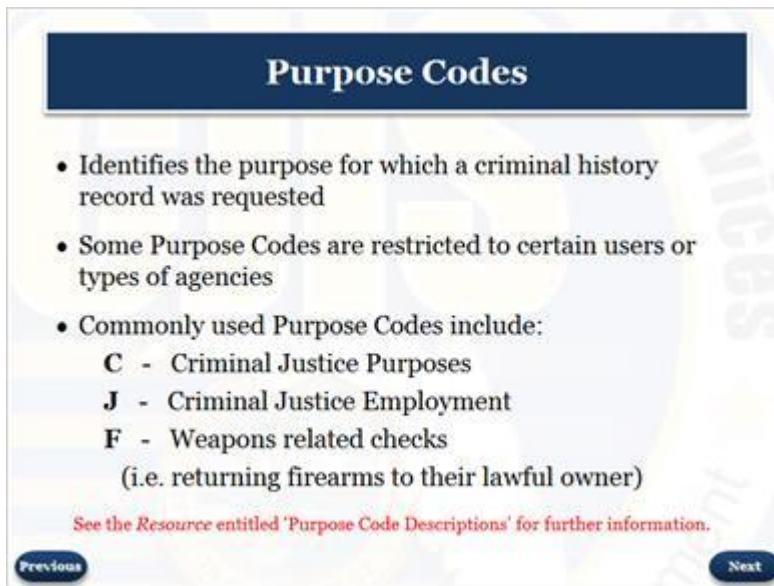
2015



- 25

Agencies may use the FCX message key with Purpose Code ‘C’ to view an XML format rap sheet by using the FDLE provided software, eAgent. The XML rap sheet provides the following: criminal history in a chronological descending order, the ability to expand or collapse different sections, special caveats such as “REGISTERED FELONY OFFENDER” at the top, and juvenile arrests records which are highlighted with pink backgrounds.

1.29 Purpose Codes



Purpose Codes

- Identifies the purpose for which a criminal history record was requested
- Some Purpose Codes are restricted to certain users or types of agencies
- Commonly used Purpose Codes include:
 - C** - Criminal Justice Purposes
 - J** - Criminal Justice Employment
 - F** - Weapons related checks
(i.e. returning firearms to their lawful owner)

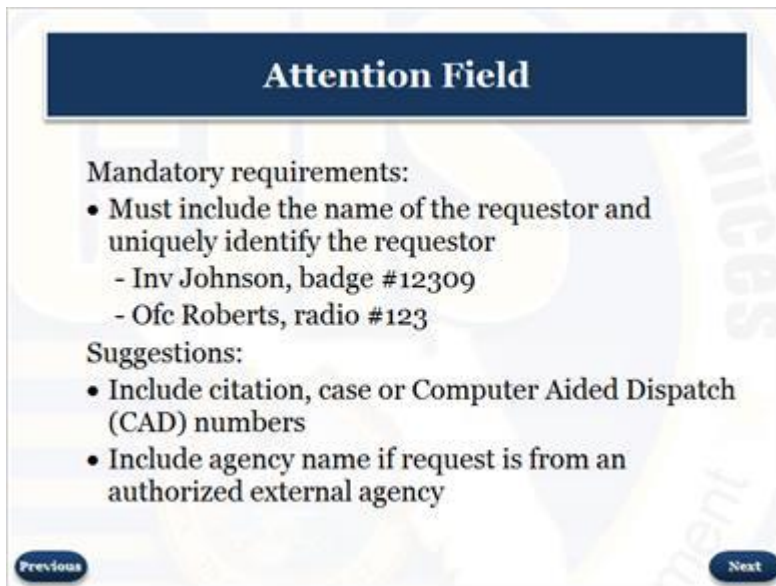
See the Resource entitled 'Purpose Code Descriptions' for further information.

Previous Next

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

1.31 Attention Field



The slide features a dark blue header with the title 'Attention Field' in white. Below the header, the text 'Mandatory requirements:' is followed by a bulleted list. The first bullet point states that the requestor's name must be included and uniquely identified, with two examples: 'Inv Johnson, badge #12309' and 'Ofc Roberts, radio #123'. Below this, the text 'Suggestions:' is followed by another bulleted list. The first suggestion is to include citation, case, or Computer Aided Dispatch (CAD) numbers. The second suggestion is to include the agency name if the request is from an authorized external agency. At the bottom left is a 'Previous' button and at the bottom right is a 'Next' button. A faint background watermark of a police badge is visible.

Attention Field

Mandatory requirements:

- Must include the name of the requestor and uniquely identify the requestor
 - Inv Johnson, badge #12309
 - Ofc Roberts, radio #123

Suggestions:

- Include citation, case or Computer Aided Dispatch (CAD) numbers
- Include agency name if request is from an authorized external agency

Previous Next

Notes:


The Attention Field is mandatory and must contain the name of the person requesting the CHRI. It is used 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.

1.32 Secondary Dissemination

Secondary Dissemination

Required if 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



Previous Next

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 information is considered secondary dissemination and should be documented on the dissemination log.

1.33 Secondary Dissemination Log

Secondary Dissemination Log

- Document the sharing of CHRI on the Secondary Dissemination Log
- Handwritten or electronic form
- Must be maintained at the agency for at least four years
- Must include the following fields of information:

Date	Subject's Name	SID or FBI Number	Requestor (released to)	Requestor Agency (released to)	Operator (released by)	Reason Disseminated	Purpose Code
------	----------------	-------------------	-------------------------	--------------------------------	------------------------	---------------------	--------------

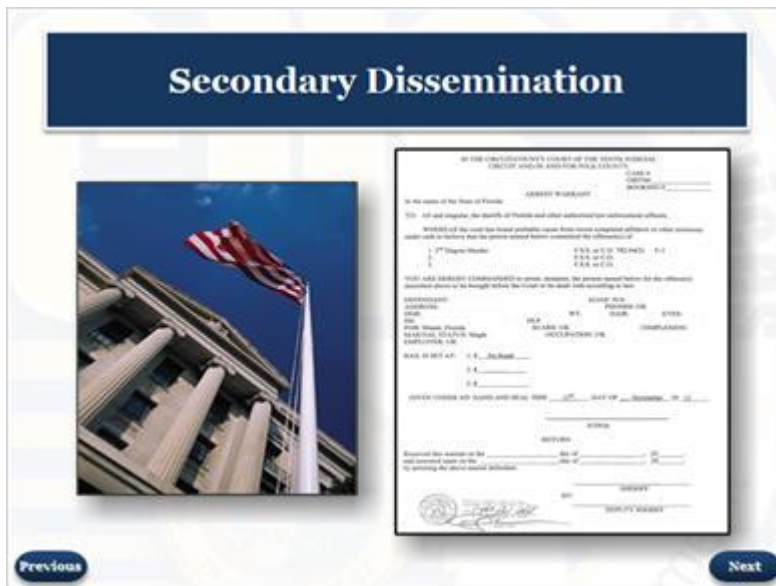
See the Resource entitled 'Sample Secondary Dissemination Log'.

Previous Next

Notes:

Users must document the sharing of CHRI on a Secondary Dissemination Log. 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 an example, please refer to the resource entitled 'Sample Secondary Dissemination Log'.

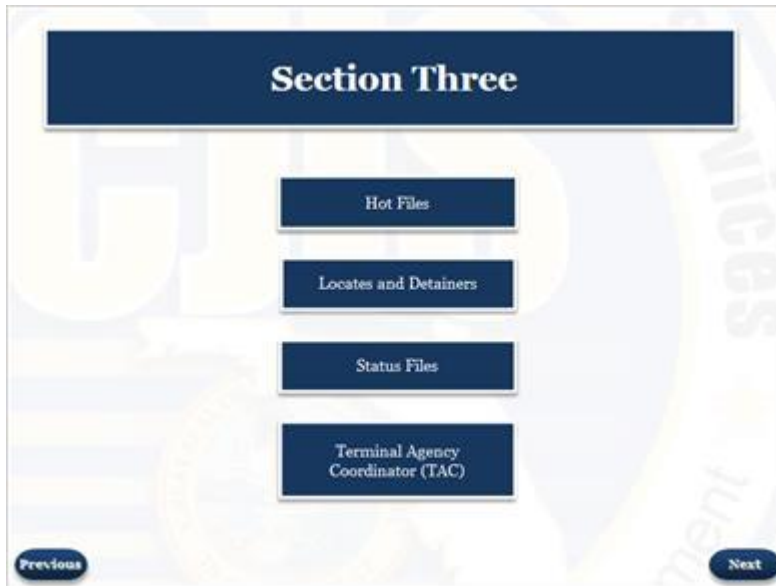
1.34 Secondary Dissemination



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.

1.36 Section Three




Notes:

Section Three of the Limited Access Certification Course includes an overview of Hot File Records, Locates and Detainers, Status Files, and the Terminal Agency Coordinator or TAC. The student will learn about Hot File records and what types of information they contain. The student will also learn about Locates and Detainers and why they are important. This section will cover the various records and information contained within Status Files and what types of Status Files are located within NCIC and FCIC systems. Included in this section will be an overview of the roles and responsibilities of the TAC.

1.37 Hot Files

Hot Files

- Records entered into FCIC/NCIC by an agency upon receiving notification that:
 - a person is wanted, missing or unidentified
 - property in question has been reported stolen, abandoned, lost or recovered
- Entries must have supporting documentation (reports, supplemental documents, etc.)
- Files are constantly being updated

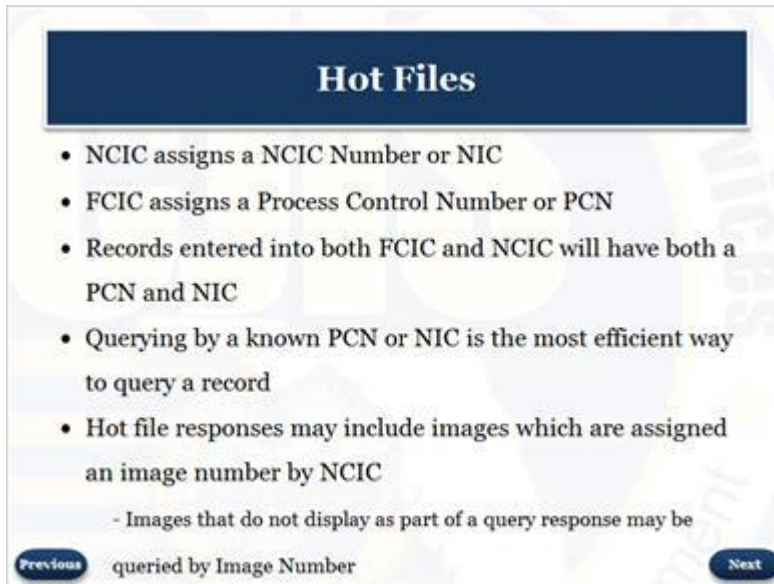


Previous Next

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. All files are constantly being updated.

1.38 Hot Files

A presentation slide titled "Hot Files" in a dark blue header. The slide contains a bulleted list of five points regarding NCIC and FCIC record management. A sub-point is listed below the main bullet points. At the bottom, there are "Previous" and "Next" navigation buttons flanking the text "queried by Image Number".

Hot Files


- NCIC assigns a NCIC Number or NIC
- FCIC assigns a Process Control Number or PCN
- Records entered into both FCIC and NCIC will have both a PCN and NIC
- Querying by a known PCN or NIC is the most efficient way to query a record
- Hot file responses may include images which are assigned an image number by NCIC
 - Images that do not display as part of a query response may be queried by Image Number

Previous Next

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. 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 not automatically displayed may be queried specifically by each individual Image Number.

1.39 Property Files Introduction

A presentation slide titled "Property Files" in a dark blue header. Below the header, a bulleted list states: "Property Files consist of the following:" followed by a list of items: Articles, Guns, Vehicles, Boats, Vehicle and Boat Parts, and Securities. At the bottom left is a "Previous" button and at the bottom right is a "Next" button. The background features a faint, large watermark of a shield with the word "UNIVERSITY" and other text.

Property Files

- Property Files consist of the following:
 - Articles
 - Guns
 - Vehicles
 - Boats
 - Vehicle and Boat Parts
 - Securities

Previous Next

Notes:

Property files include the following records: articles, guns, vehicles, boats, vehicle and boat parts, and securities. The 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.

1.40 Property Files

A presentation slide titled "Property Files" in a dark blue header. The slide features three images on the left: a diamond, a handgun, and a stack of US dollar bills. To the right of these images is a bulleted list. At the bottom left is a "Previous" button and at the bottom right is a "Next" button.

- Articles
- Guns
 - Serial numbers are not unique
- Securities
 - NCIC only record

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.

Stolen toxic, hazardous materials are also available in the Article File.



The Gun File contains weapons that expel a projectile by air. An exception is BB 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 stolen, embezzled, used for ransom or counterfeited.

1.41 Property Files

Property Files



- Vehicles
 - Stolen License Plates
- Boats
- Vehicle and Boat Parts

[Previous](#)[Next](#)

Notes:

Vehicle File responses 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. Note: A query into the Vehicle File and a query for vehicle registrations are two different transactions and performed differently for in-state and out-of-state vehicles.

Boat responses 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.

1.42 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.

1.43 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

[Previous](#)[Next](#)

Notes:

Wanted Person records include any individual 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.

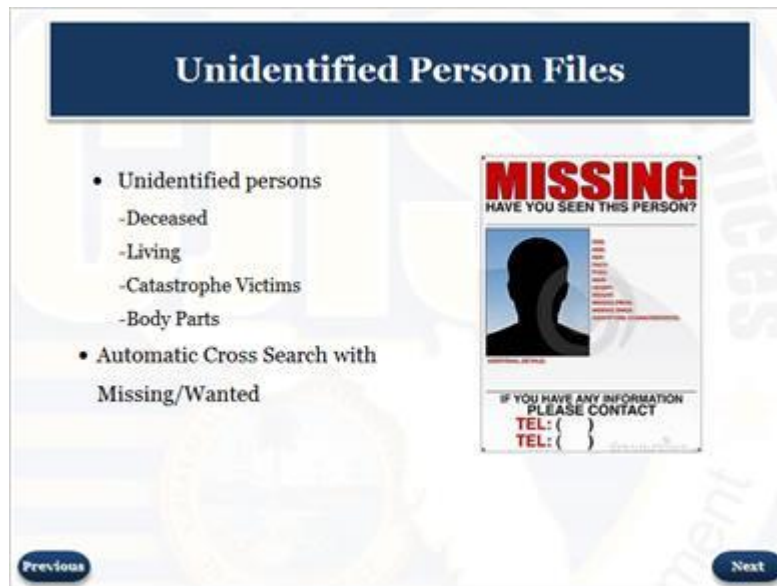
2015



39

Additionally, the International Criminal Police Organization (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.

1.45 Unidentified Person Files



Notes:

According to Florida Statute 406, 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 the following:

- Deceased: A person who is no longer living for whom the identity cannot be ascertained.
- Living: A person who is living and unable to ascertain his/her identity (e.g., infant or amnesia victim). The information on unidentified living persons should only be included if the person gives his/her consent or if they are physically or mentally unable to give consent.
- Catastrophe Victim: A person who is a victim of a catastrophe for whom the identity cannot be ascertained.
- Body Parts: Body parts may be entered as deceased, when a body has been dismembered, or as the result of a catastrophe.

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

1.47 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: 19600806	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 for special handling instructions
- Violations could result in an arrest such as Writs of Bodily Attachment for failure to pay child support

[Previous](#)[Next](#)

Notes:

When conducting a person query, Status Files may be returned in addition to the Wanted and Missing Person responses. Status File records are for informational purposes. However, violations of certain conditions of Status File records could result in an arrest such as Writs of Bodily Attachment for failure to pay child support.

1.48 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 Offender
- FL Gang Records
- Writs of Bodily Attachment
- Florida Deported Alien

CRIMINAL GANG MEMBER (FLORIDA STATEWIDE INTELLIGENCE SYSTEM - INSITE)

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:
DOB: 19330303	ENTRY DATE: 09/29/201
RACE: BLACK	PCN: T200090952
SEX: MALE	NIC: NONE
SOC SEC NO: 000000000	
LIC PLATE: 123INTEL	LIC ST: FL LIC YR: 2000
LIC TYPE: REGULAR PASSENGER AUTOMOBILE PLATE	
VIN: WDCYCT8F8M300007	VEH YEAR:
CASE NO: 54854	
ENTERING MNE: 037010081	
ENTERING AGY: FL0370142 - FDLE - TALLAHASSEE	
NOTIFY AGY: NO NOTIFY PUBLICLY AVAILABLE	

[Previous](#)[Next](#)

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, and the Florida Deported Alien File. These records will only have a PCN assigned.

1.49 NCIC-Only Status Files



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, National Sex Offender Registry, the NCIC Gang file, Protective Interest, the 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.

1.50 Status Files in both FCIC and NCIC

Status Files in both FCIC and NCIC

- Sexual Predators/Sexual Offenders
- Domestic Violence Injunctions (both active and historical)
- Florida Department of Corrections Probation/Parole records



[Previous](#)[Next](#)

Notes:

Status Files contained in both FCIC and NCIC include the Sexual Predator/Offender File, Domestic Violence Injunctions, and the Florida Department of Corrections Probation and Parole records. These records will have both a PCN and NIC assigned.

1.51 Person File Responses

Person File Responses

- Responses may include any or all of the records contained in the person files (wanted, missing and status)
- Search is expanded or narrowed based on information/data entered as search criteria
- Carefully review all responses received; responses received may not match the person searched

See the Resource entitled 'Best Practices for Person Searches' for further information.

Previous Next

Notes:

When a user queries the Person Files, 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.

Please see the resource entitled “Best Practices for Person Searches” for further information on person queries.

1.52 Hits

Hits

- Hit - a 'positive response'
- 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
- The Hit confirmation process must be completed prior to taking action



[Previous](#)[Next](#)

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 or recover stolen property depending on the circumstances.

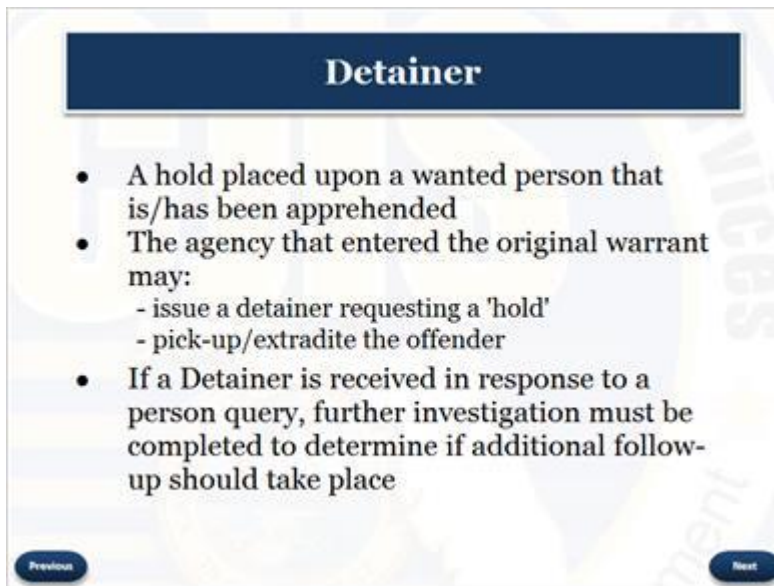
Hit Confirmation time limits are set according to the level of priority assigned by the requesting agency. Urgent hit confirmation requests require a ten minute response, while Routine hit confirmation requests must be responded to within one hour. While Hit Confirmation responses are handled by Full Access operators, users should realize that the hit confirmation process must be completed prior to taking action on a hit.

2015



47

1.54 Detainer



Detainer

- A hold placed upon a wanted person that is/has been apprehended
- The agency that entered the original warrant may:
 - issue a detainer requesting a 'hold'
 - pick-up/extradite the offender
- If a Detainer is received in response to a person query, further investigation must be completed to determine if additional follow-up should take place

Previous Next

Notes:

A detainer is an electronic hold on a person that is or has been apprehended. The agency that entered the warrant may issue a detainer requesting that the person be held until the arresting agency's 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.

1.56 *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 Kathy, 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 sure what to report to the detective."

[illegible]

"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 TAC." 10-4, 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".

1.59 Terminal Agency Coordinator

Terminal Agency Coordinator (TAC)

- Agency's main CJIS point of contact
- Liaison with FDLE as it relates to FCIC/NCIC
- Ensures agency user compliance for FCIC/ NCIC, and Nlets systems

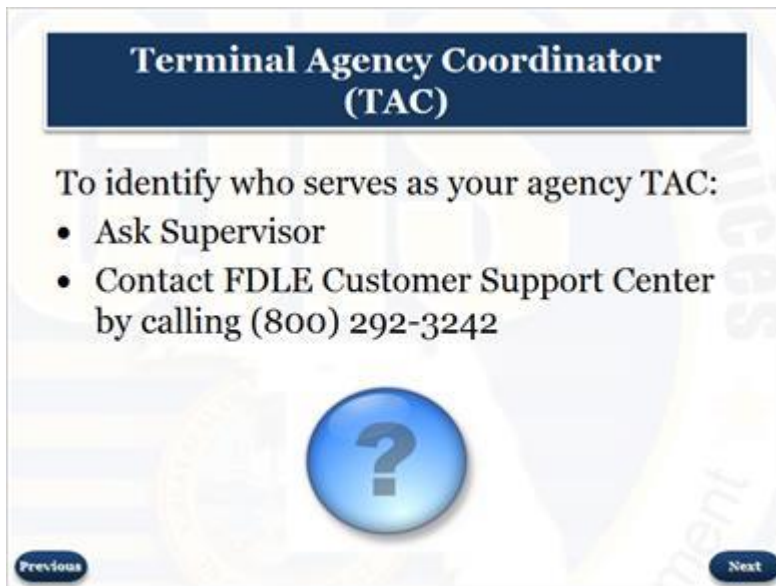


[Previous](#)[Next](#)

Notes:

The Terminal Agency Coordinator or TAC serves as an agency's main point of contact both internally and externally in CJIS matters regarding FCIC/NCIC. The TAC also serves as the liaison between the local agency and FDLE in CJIS matters involving these systems. The TAC 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.

1.60 Terminal Agency Coordinator



**Terminal Agency Coordinator
(TAC)**

To identify who serves as your agency TAC:

- Ask Supervisor
- Contact FDLE Customer Support Center by calling (800) 292-3242

A large blue circular button with a white question mark is centered below the list. At the bottom left is a 'Previous' button and at the bottom right is a 'Next' button. The background features a faint Florida Department of Law Enforcement seal.

Notes:

Do you know who serves as the TAC and Alternate TAC for your agency? If you don't know you can ask your supervisor or call the FDLE customer support center at (800) 292-3242.

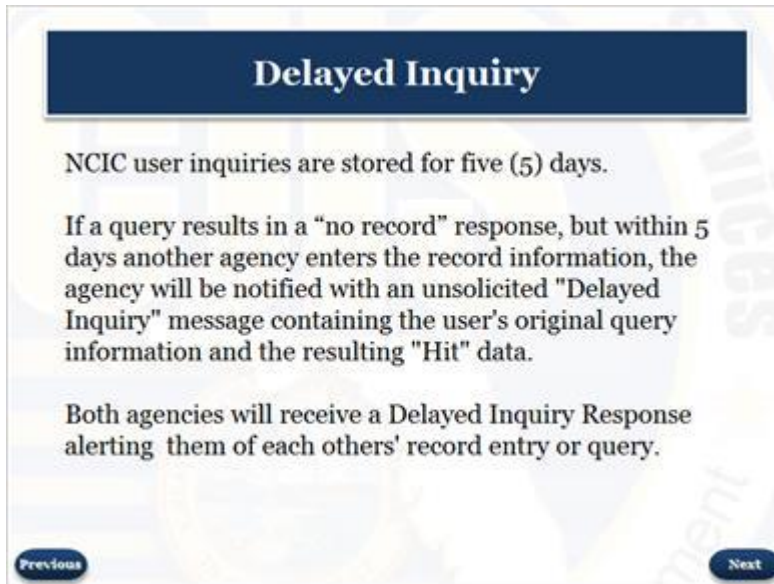
1.61 Section Four



Notes:

Section Four of the Limited Access Certification Course includes an overview of Delayed Inquiries and the different type of Alerts issued by law enforcement agencies regarding missing and/or endangered children or adults, and alerts regarding endangered law enforcement officers. Next, there will be an overview of Concealed Weapon Permits and how to query in-state and out-of-state concealed weapon permit records. Additionally, the student will learn about various systems or Investigative Tools available to law enforcement that maintain archived information useful for investigations.

1.62 Delayed Inquiry



Delayed Inquiry

NCIC user inquiries are stored for five (5) days.

If a query results in a “no record” response, but within 5 days another agency enters the record information, the agency will be notified with an unsolicited "Delayed Inquiry" message containing the user's original query information and the resulting "Hit" data.

Both agencies will receive a Delayed Inquiry Response alerting them of each others' record entry or query.

[Previous](#) [Next](#)

Notes:

NCIC user inquiries 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 roadside stop made on a stolen vehicle prior to it being entered as stolen would trigger a notification to both the entering and querying agencies after the entry is made.

1.63 Example of Delayed Inquiry



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.

1.64 System Identifiers

System Identifiers

- **Originating Agency Identifier (ORI)**
 - assigned by the Federal Bureau of Investigation (FBI)
 - used to identify out of state agencies and specific devices for NCIC/Nlets transactions
 - also used for all Hit Confirmation transactions
- **Mnemonics**
 - assigned by the Florida Department of Law Enforcement (FDLE)
 - identifies both the agency and the specific device in Florida for FCIC transactions

Previous Next

Notes:

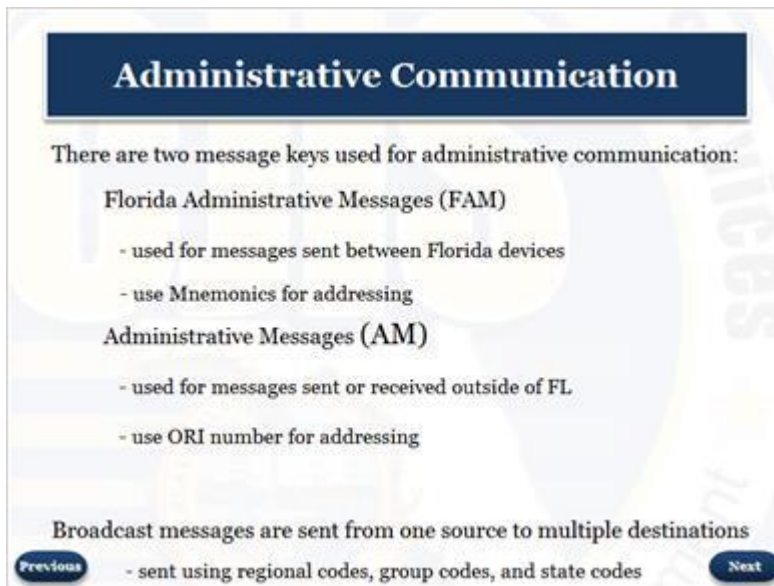
FCIC, NCIC and Nlets use system identifiers to indicate the source or destination of electronic transactions.

The FBI assigns Originating Agency Identifiers, or ORIs. Each agency is issued a primary ORI number, and devices or groups of devices within the agency are also assigned ORIs. These alphanumeric identifiers are used for NCIC and Nlets transactions, as well as hit confirmations identifying the agency in the transaction.

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.

1.65 Administrative Communication



Administrative Communication

There are two message keys used for administrative communication:

- Florida Administrative Messages (FAM)**
 - used for messages sent between Florida devices
 - use Mnemonics for addressing
- Administrative Messages (AM)**
 - used for messages sent or received outside of FL
 - use ORI number for addressing

Broadcast messages are sent from one source to multiple destinations

[Previous](#) - sent using regional codes, group codes, and state codes [Next](#)

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.

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. For further information please see the resource entitled 'Administrative Communication'.

1.66 Guidelines for Communication

Guidelines for Communication

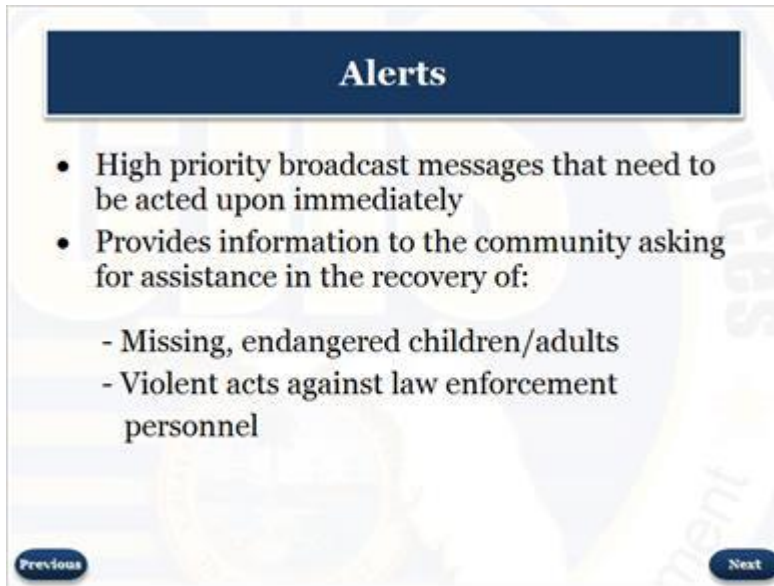
- Use plain English
 - NO 10 codes or signal codes
- Should not be used frivolously
 - NO personal messages or holiday greetings
 - NO job or retirement announcements
 - NO press releases
- Include a signature which clearly identifies the agency and operator
- Respond to messages in a timely manner

Previous Next

Notes:

Users must follow basic guidelines when sending administrative communication. These include using plain English and not sending non law enforcement related messages such as personal messages or 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.

1.67 Alerts Introduction

A presentation slide titled "Alerts" in a dark blue header. The slide contains a bulleted list of information. At the bottom left is a "Previous" button and at the bottom right is a "Next" button. The background features a faint, large watermark of the Seal of the Commonwealth of Massachusetts.

Alerts

- High priority broadcast messages that need to be acted upon immediately
- Provides information to the community asking for assistance in the recovery of:
 - Missing, endangered children/adults
 - Violent acts against law enforcement personnel

Previous Next

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.

1.68 Types of Alerts



The slide is titled "Types of Alerts" in a dark blue header. It is divided into two main sections. The top section features the "FLORIDA AMBER Alert PLAN" logo on the left and a text box on the right that reads: "AMBER Alerts - High priority message issued when a child has been abducted and is endangered". The bottom section features a text box on the left that reads: "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". To the right of this text is a logo for the "Missing Endangered Persons Information Clearinghouse" with the text "FLORIDA DEPARTMENT OF LAW ENFORCEMENT" below it. At the bottom left is a "Previous" button and at the bottom right is a "Next" button.

Types of Alerts

FLORIDA AMBER Alert PLAN

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

Missing Endangered Persons Information Clearinghouse
FLORIDA DEPARTMENT OF LAW ENFORCEMENT

Previous Next

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.

1.69 Types of Alerts



The slide is titled "Types of Alerts" in a dark blue header. Below the header is the Florida Silver Alert Plan logo, which includes a stylized eye icon and the text "Florida Silver ALERT PLAN", "1-888-FL Missing (356-4774)", and "Florida Department of Law Enforcement". The main text defines Silver Alerts and lists two types: State and Local. At the bottom are "Previous" and "Next" navigation buttons.

Types of Alerts

Florida Silver ALERT PLAN
1-888-FL Missing (356-4774)
Florida Department of Law Enforcement

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

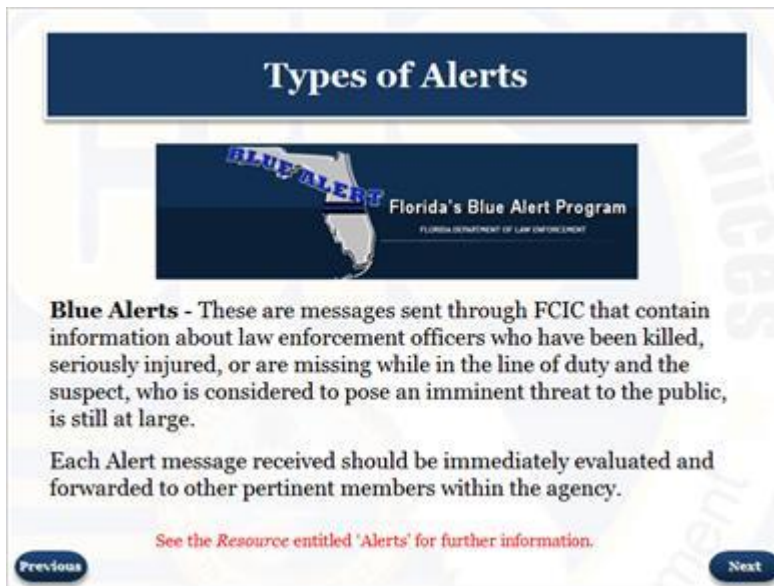
- For State Silver Alert: Person must be in an identified vehicle
 - FDLE assists with the FCIC Broadcast Message, media, public and roadside message alerts
- For Local Silver Alert: Person must be on foot
 - Local agency is responsible for FCIC Broadcast Message, media and public alerts

Previous Next

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.

1.70 Types of Alerts



The slide is titled "Types of Alerts" in a dark blue header. Below the header is a graphic for "Florida's Blue Alert Program" featuring a map of Florida with a blue alert banner and the text "FLORIDA DEPARTMENT OF LAW ENFORCEMENT". The main text describes Blue Alerts as messages sent through FCIC regarding law enforcement officers who have been killed, seriously injured, or are missing while in the line of duty, and the suspect poses an imminent threat to the public. It also states that each alert message should be immediately evaluated and forwarded to other pertinent members within the agency. At the bottom, there is a red text prompt to see the resource entitled 'Alerts' for further information, and "Previous" and "Next" navigation buttons.

Types of Alerts



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 entitled 'Alerts' for further information.

Previous Next

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 Florida Fusion Center. Please refer to the resource entitled "Alerts" for further information regarding the activation of Amber, Missing Child, Silver and Blue Alerts.

1.72 Concealed Weapon Permit Query

Concealed Weapon Permit Query

- Searchable by FL permit/ license number
- may be searched by SSN, if available

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

SAMPLE

DOB: JOHN E.
11 SAMPLEVILLE AVENUE
BOON, BARRY, FL 32000

BIRTH DATE	MM/DD/YYYY	SEX	M	RACE	W
ISSUANCE NUMBER	123456789	ISSUANCE DATE	MM/DD/YYYY	EXPIRATION DATE	MM/DD/YYYY
ISSUANCE NUMBER	123456789	ISSUANCE DATE	MM/DD/YYYY	EXPIRATION DATE	MM/DD/YYYY

This document is not valid unless it is signed by the Department of Agriculture and Consumer Services, Division of Licensing and Registration, under Section 120.05, Florida Statutes.

John E. Sample
GOVERNOR
SECRETARY OF STATE

[Previous](#)[Next](#)

Notes:

Concealed weapon permits 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. Finally, the concealed weapon permit search is restricted only to users at a law enforcement agency in connection with the performance of lawful duties.

1.73 Concealed Weapon Permit Query

Concealed Weapon Permit Query

- Certain states provide automated responses to concealed weapon permit queries



Please refer to www.nlets.org for a current map of states that respond to the concealed weapon permit query.

Previous Next

Notes:

Nlets also allows for out-of-state concealed weapon permit queries. Please refer to www.nlets.org for a current map of states that respond to the out of state concealed weapon permit query.

1.74 Investigative Tools

A presentation slide titled "Investigative Tools" in a dark blue header. The slide contains two bullet points: "Various systems available to criminal justice users maintain a log of queries & responses:" with sub-points "- FCIC" and "- NCIC"; and "Archived information contained in these logs can be used for:" with sub-points "- Criminal investigations" and "- Administrative purposes". To the right of the second bullet point is an illustration of a magnifying glass. At the bottom, a red line of text says "See the Resource entitled 'Investigative Tools' for further information." Below this are two blue buttons labeled "Previous" and "Next".

Investigative Tools

- Various systems available to criminal justice users maintain a log of queries & responses:
 - FCIC
 - NCIC
- Archived information contained in these logs can be used for:
 - Criminal investigations
 - Administrative purposes

See the Resource entitled 'Investigative Tools' for further information.

Previous Next

Notes:

Many databases utilized by criminal justice agencies maintain a log of queries and responses. FCIC and NCIC maintain archived information which can then be used in criminal investigations or for administrative purposes. To obtain transaction log information for FCIC contact FDLE. For NCIC transactions contact the FBI. Please refer to the resource entitled "Investigative Tools" for further information.

1.75 Transaction Archive Report (TAR)

Transaction Archive Report (TAR)

- Off-line system or Transaction Archive Report (TAR)
- TARs may be used for:
 - criminal investigations
 - misuse investigations

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 00558893 QV S13004462 O
<HDR>: [UCD]: DEV: 00001 [MNE]: S13004462 [HIT]
[CTL]: 105874
[IAP]:
[DATE]: 20120621 [TIME]: 1226 [NBR]: 00520
<MNE>: QV
<DR>: FL01308M0
<LIC>: 8327JR
<LIS>: FL
-ERROR-
UNKNOWN USER CODE PLEASE NOTIFY TAC
-END-

[Previous](#)[Next](#)

Notes:

All transactions run through FCIC are maintained in an off-line system called the Transaction Archive Report or TAR. TARs may be requested from FDLE and can be used for criminal and misuse investigations. To request a TAR send an email to TARRequest@fdle.state.fl.us.

1.76 Section Five



Notes:

Section five is the Security Awareness portion of the Limited Access Certification Training Course. The FBI CJIS Security Policy provides Criminal Justice Agencies and Noncriminal Justice Agencies with a minimum set of security requirements for access to the Federal Bureau of Investigation CJIS Division systems and how to protect and safeguard Criminal Justice Information.

1.77 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
- Disciplinary actions can result in criminal and/or civil prosecution



[Previous](#)[Next](#)


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.

1.78 System Vulnerabilities and Threats

System 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

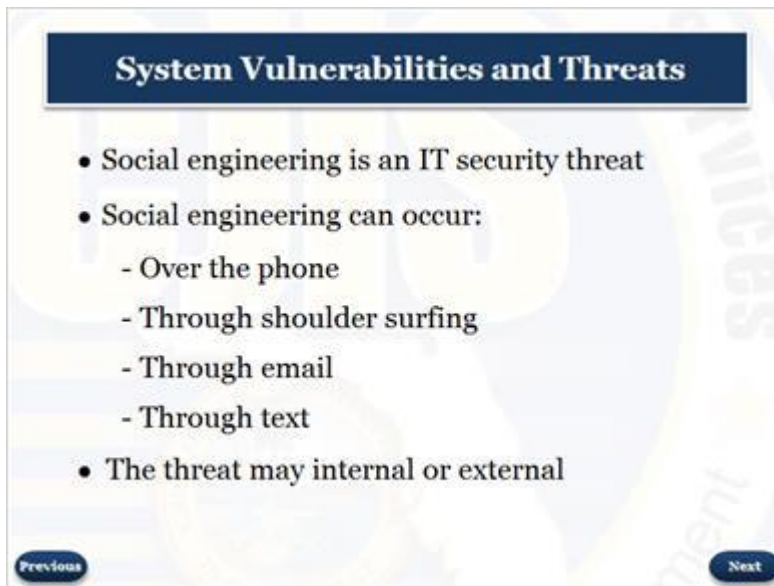


Previous Next

Notes:

One of the greatest threats to an agency's Information Technology (IT) system is from users within the agency. 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.

1.79 System Vulnerabilities and Threats



System Vulnerabilities and Threats

- Social engineering is an IT security threat
- Social engineering can occur:
 - Over the phone
 - Through shoulder surfing
 - Through email
 - Through text
- The threat may internal or external

Previous Next

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 IT system, or it can be as simple as shoulder surfing, someone looking over your shoulder to get your password. Either way social engineering is a viable and real threat that can occur either internally or externally.

1.80 Access Security

A presentation slide titled "Access Security" in a dark blue header. The slide contains a bulleted list of four points on the left and a graphic on the right. The graphic shows the word "security" in a blue, glowing font over a dark background with a fingerprint pattern. At the bottom left is a "Previous" button and at the bottom right is a "Next" button.

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

Previous Next


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 change to a position and no longer require access.

1.81 User Accountability

User Accountability

- Users can 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



[Previous](#)[Next](#)

Notes:

Users can 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 to another agency is allowed only to authorized recipients using secure devices.

1.82 User Accountability

Use of Acknowledgement Statement

- Each user is accountable for the access and use of CJI
- Prior to accessing a CJI 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

Previous Next

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.

1.84 Handling of Criminal Justice Information (CJI)

Handling of Criminal Justice Information (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 (preferably 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

Previous Next

Notes:

Agencies and their users must ensure electronic media and printed documents that contain criminal justice information, whether in transit or storage, is properly secured. Electronic criminal justice information must be protected and preferably encrypted. 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 FTP, make sure 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 TAC or Local Agency Security Officer, or 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.

1.85 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

Additionally 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



Previous

Next

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

1.86 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 to:

- 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

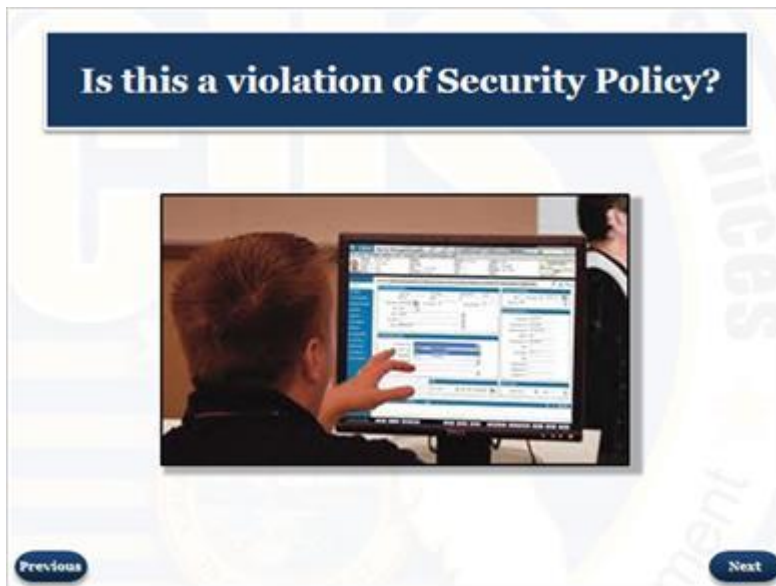
Previous Next

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.

1.87 Is this a violation of Security Policy?




Notes:

Is this a violation of the Security Policy? It is the graveyard shift at the intake desk of a jail. One supervisor and an employee who has just returned from vacation are scheduled to work. 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 the jail management system and discovers his CJIS 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 first opportunity, the intake employee decides to use the login credentials of a fellow worker who keeps her password written down at her workstation.

1.89 Physical Security

Physical Security



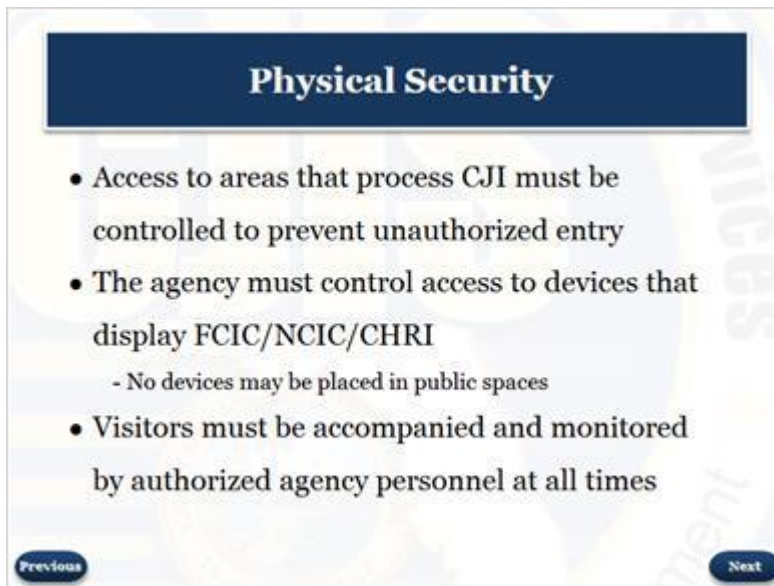
- Devices accessing FCIC/NCIC must be placed in a controlled area
- Screens must be protected from routine viewing by unauthorized personnel
- Authorized personnel must accompany all visitors to computers centers and/or workstation areas at all times
- Persons that make contact with an agency requesting protected information should be challenged

Previous Next

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 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 TAC. Persons that make contact with 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) and dispatch computers located in a physically secure location are exempt from this requirement.

1.90 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

Previous Next


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 to the agency must be accompanied and monitored by authorized agency personnel at all times in CJIS Security Policy defined secure locations and areas where CJI is being processed.

1.91 Network and Desktop Security

Network and Desktop Security

- Virus protection software installed and regularly updated
- Agencies should implement spam and spyware protection, as well as advanced authentication, and encryption controlled interfaces
- Users should work with agency IT staff to minimize data loss



[Previous](#)[Next](#)


Notes:

All computers accessing FCIC/NCIC or the CJNet must have virus protection software installed and regularly updated. This software is used to protect the computer from Viruses, Worms, Trojan Horses and other malicious codes. Agencies should implement spam and spyware protection, as well as advanced authentication, and encryption controlled interfaces such as firewalls, gateways, and routers to protect criminal justice information. Users should be cautious when opening email attachments from unknown senders. These attachments could contain viruses and other malicious codes intended to cause harm. Also, users should work with agency IT staff to minimize data loss caused by inconsistent or poor power supplies.

1.92 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



[Previous](#)[Next](#)

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 should have all of their security features enabled and special reporting procedures should be in place. These procedures include loss of device control; total device loss or device compromise whether in or outside of the United States.

1.93 Non-Agency Issued Device Security

Non-Agency Issued Device Security



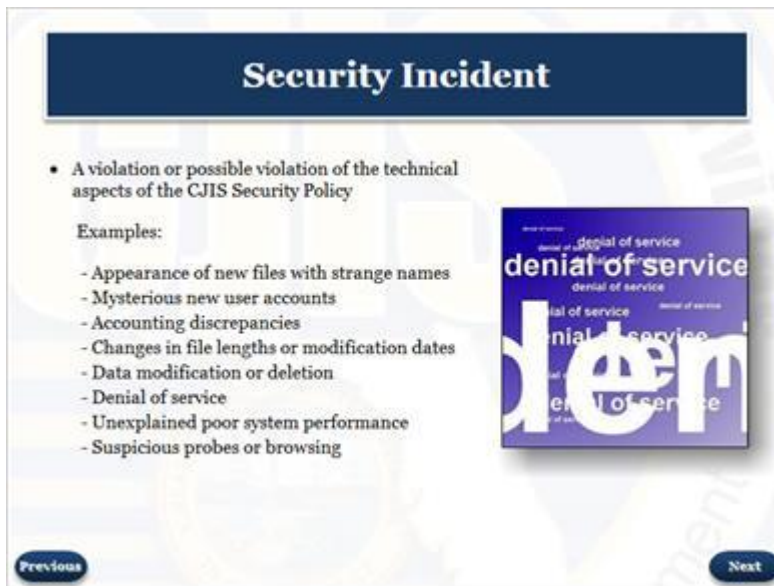
- Personally owned equipment and software shall not be authorized to access, process, store or transmit CJI unless the agency has established and documented the specific terms and conditions
- Utilizing publicly accessible computers to access, process, store or transmit CJI is prohibited

Previous Next

Notes:

Personally owned equipment and computer software shall not be authorized to access, process, store, or transmit criminal justice information unless the agency has documented the specific terms and conditions for personally owned information system usage. 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 prohibited.

1.94 Security Incident



Security Incident

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

Examples:

- 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
- Suspicious probes or browsing

The slide also features a graphic on the right side showing the words 'denial of service' repeated in a stylized, overlapping manner. At the bottom left is a 'Previous' button and at the bottom right is a 'Next' button.

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; and suspicious probes or browsing.

1.95 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 CJIS Information Security Officer (ISO) for FDLE

Previous Next

Notes:

Users may only see indicators of a security incident and should follow their agency's written policy describing actions to be taken during an FCIC/NCIC or CJNet security incident. The operator should 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 CJIS Information Security Officer.

1.96 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?

1.98 Agency's Security Responsibility

Agency's Security Responsibility

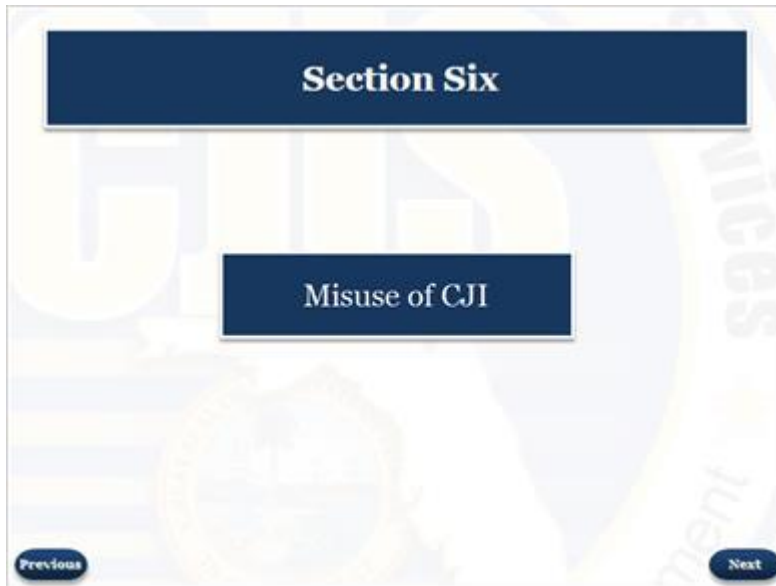
- The agency shall approve individual access privileges and shall enforce physical and logical access restrictions
- The agency shall enforce the most restrictive set of rights/privileges or access needed by users
- The agency shall implement least privilege access based on specific duties, operations 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

Previous Next

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.

1.99 Section Six



Notes:

Section Six will address issues related to the misuse of FCIC and NCIC. This section will offer examples of common types of misuse and provide statutory guidance for penalties if misuse occurs.

1.100 Misuse of Criminal Justice Information (CJI)

Misuse of Criminal Justice Information (CJI)

- F.S. 112 sets forth the expectations of public employees behavior and ethics
- Ethics is described as the rules or 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

Previous Next

Notes:

F.S. 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.

1.101 Misuse of Criminal Justice Information (CJI)

Criminal Justice Purposes

- The CJI, PII and CHRI information can only be used/disseminated in the administration of criminal justice duties
- The term "administration of criminal justice" is defined in Section 943.045(2), Florida Statutes and includes performing functions of:
 - Detection
 - Adjudication
 - Apprehension
 - Correctional Supervision
 - Detention
 - Rehabilitation of accused persons
 - Pre-trial release
 - Criminal identification activities
 - Post-trial release
 - Prosecution
- Users should be aware that improper handling of CJI, PII and CHRI information is a violation of policy and could result in criminal prosecution.

Previous Next

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. 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. Information contained in any CJIS system from other state computer files shall only be used for criminal justice purposes as authorized by Florida Statute.

1.102 Misuse of Criminal Justice Information (CJI)

Misuse of Criminal Justice Information (CJI)

- Any access of CJI systems and/or dissemination of information obtained for non-criminal justice purposes is 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

Previous Next

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 agency assigned work-related purposes.

1.103 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



Previous

Next

Notes:

Any access and/or dissemination of information from criminal justice information systems for non-criminal justice purposes are considered misuse of the system. 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.

1.104 Examples of Misuse

Examples of Misuse

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

Previous Next

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.

1.106 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 entitled 'Misuse' for further statutes related to penalties regarding the misuse of CJI.

Previous Next

Notes:

The following are Florida Statutes which address 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 benefitting 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 entitled "Misuse".

1.107 You are Ready to Test



To Complete Training

The modular portion of the training has finished. To record completion of the training please click on the picture below to be re-directed to the nexTEST application.

nexTEST
CJIS TESTING

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

Previous

Notes:

You have completed the modular portion of the Limited Access Certification Course. To record completion of the training you must click on the nexTEST picture to be re-directed to the nexTEST application.

Limited Access users may begin the Limited Access Certification test immediately, or return to nexTEST to complete the exam within fourteen (14) days. Full Access users must now complete the Full Access Online Certification training prior to taking the certification exam.