Security and Privacy Training – General User

Welcome to the CJIS Security and Privacy Training! This training is designed for users with the authorization to use an information system.

This training will cover the following topics:

- Introduction
- Literacy Training and Awareness
- Roles and Responsibilities
- What is CJI?
- Proper Access, Use, & Dissemination of CJI
- Access Control
- Physical Security
- System Security
- Incident Response
- Conclusion

Introduction

Security and Privacy Training

All personnel whose duties require them to have unescorted access to a physically secure location that processes or stores Criminal Justice Information (CJI) must complete Security and Privacy training.

The FBI CJIS Security Policy requires that all personnel fitting the above criteria must complete this training:

- ***Before*** authorizing access to the system, information, or performing assigned duties
- ***Every year*** after the initial training

Training Record Retention

FBI Security Policy requires that all training records must be kept current and be maintained for a minimum of ***three years*** by the Federal, State, or Local Agency.

Literacy Training and Awareness

Security and Privacy Literacy

Security and privacy literacy is the understanding of the threats, vulnerabilities, and risks associated with security and privacy. It is also about the actions necessary for users to maintain security and personal privacy and to respond to suspected incidents.

Literacy training must be taken at the following times:

- ***Before*** accessing CJI
- ***Every year*** after the initial training
- ***Within 30 days*** of any security event for all users involved in the event
- When required by system changes

After the initial training, subsequent literacy training may be satisfied by one or more short ad hoc sessions and include topical information on recent attack schemes, changes to organizational security and privacy policies, revised security and privacy expectations, or a subset of topics from the initial training.

Threats to Security and Privacy

A **security threat** is any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, or denial of service.

Examples of Threats

- Natural (lightning, heat, or water)
- Intentional (someone wanting to cause harm on purpose)
- Unintentional (a user accidentally erasing a critical file while "playing" on the computer)

One of the greatest threats to an agency's security, whether intentional or unintentional, is **its own personnel**!

Insider Threat

Having proper security measures against the insider threat is a critical component of CJIS Security. Potential indicators and possible precursors of insider threat can include behaviors such as:

- Inordinate, long-term job dissatisfaction
- Attempts to gain access to information not required for job performance
- Unexplained access to financial resources
- Bullying or harassment of fellow employees
- Workplace violence
- Other serious violations of policies, procedures, directives, regulations, rules, or practices

Social Engineering and Mining

Social engineering is an attempt to trick an individual into revealing information or taking an action that can be used to attack systems or networks. **Social mining** is an attempt to gather information about the organization that may be used to support future attacks.

Examples of commonly used types of social engineering

- **Phishing** is a digital form of social engineering that uses authentic-looking emails to trick users into sharing personal information. It usually includes a link that takes the user to a fake website. If you cannot verify the source, do not open the link. Report suspicious messages to your IT team.
  - **Spear Phishing** is a type of phishing where a specific user or group of users is targeted because of their position (such as a company's administrators).
- **Social media exploitation** is where the attacker uses information found on a user's social media profiles to create targeted spear phishing attack.
- **Pretexting** and **Impersonation** is where the attacker creates a fictional backstory that is used to manipulate someone into providing private information or to influence behavior. Attackers will often impersonate a person of authority, co-worker, or trusted organization to engage in back-and-forth communication prior to launching a targeted spear phishing attack.
  - **Fake IT Support calls** are a common form of impersonation where someone pretends to be an authorized user or administrator in an attempt to gain illicit access to protected data systems. The person has enough information to sound credible, and they ask the user for some bit of information that allows the attacker to gain access to the desired system.
- **Baiting** is the use of a false promise to lure the user into a trap, including enticing ads that lead to malicious sites or encourage users to download a malware-infected application.
  - **Scareware** is a type of baiting where the use of false alarms or fictitious threats lure the user into a trap. One example is the attacker convincing a user that their system is infected with malware and that they should install software granting remote access. Another example is that the attacker claims to have sensitive videos which will be released if the user does not pay.
  - **Quid pro quo** is a type of baiting where the attacker requests the exchange of some type of sensitive information such as critical data, login credentials, or monetary value in exchange for a service. For example, a user might receive a phone call from the attacker who, posed

    - as a technology expert, offers free IT assistance or technology improvements in exchange for login credentials.
- **Tailgating**, also known as "piggybacking", is where an unauthorized person manipulates their way into a restricted area, such as impersonating a well-known role (e.g., delivery driver or custodian worker) or asking a user to "hold the door".
    - **Thread-jacking** is a type of digital tailgating where the attacker replies to an existing email exchange, inserting themselves into a legitimate conversation.

Shoulder Surfing

Shoulder surfing is where an unauthorized person stands near a user to get the user's password or other data from the computer monitor.

Users should take the following precautions to prevent shoulder surfing:

- Angle your computer so that other people cannot see what you are typing
- Use a privacy screen to make your screen less visible to others
- If possible, sit or stand with your back to a wall when entering a password on a device in public
- Try to avoid viewing restricted information in public
- Shield forms from viewing when filling out paperwork
- Use strong passwords to make it more difficult for someone to try and guess what you typed
- Remember to lock your computer or device when you leave your desk

Security and Privacy Vulnerabilities

A **vulnerability** is any weakness in (or absence of) security procedures, technical controls, physical controls, or other controls that could be exploited by a security threat.

Examples of Vulnerabilities

- Physical (the placement of a computer in a non-secure location)
- Natural (a server connected to a power source without a surge protector or backup power supply)
- Hardware (a connection to the internet without a firewall)
- Software (not updating the computer operating system when updates are issued)

Criminal justice data systems and networks that are interconnected to one another and the internet are especially vulnerable to exploitation by unauthorized individuals.

Minimize Vulnerability

To minimize vulnerabilities, agencies should:

- Take steps to protect against viruses, worms, trojan horses, and other malicious code by keeping antivirus software up to date
- Monitor user activity to ensure improper use is prohibited
- Challenge strangers or report unusual activity around CJI

Additionally, organizations should establish channels through which employees and management can communicate concerns regarding potential indicators of insider threat or potential instances of social engineering and data mining in accordance with established policies and procedures.

Security Alerts and Advisories

As a part of ongoing security awareness, agencies should:

- Receive information system security alerts/advisories on a regular basis
- Issue alerts/advisories to appropriate personnel
- Document the types of actions to be taken in response to security alerts/advisories
- Take appropriate actions in response
- Employ automated mechanisms to make security alert and advisory information available throughout the agency as appropriate

Roles and Responsibilities

Agency Definitions and Roles

- **CJIS Systems Agency (CSA)** is the agency responsible for establishing and administering an information security program throughout their user community, including local levels. There is only one CSA per state or federal organization.
  - **CJIS Systems Officer (CSO)** is an individual located within the CSA responsible for the administration of the CJIS network within the organization.
  - **Information Security Officer (ISO)** serves as the security point-of-contact to the FBI CJIS Division. The ISO is also responsible for documenting and providing assistance for implementing security-related controls within the organization.
- **Criminal Justice Agency (CJA)** is a governmental agency that performs the administration of criminal justice pursuant to a statute or executive order. Examples include courts, prisons, state and federal inspector general offices, police departments, etc.
  - **Terminal Agency Coordinator (TAC)** serves as the point-of-contact at the local agency for matters relating to CJIS information access.
- **Noncriminal Justice Agency (NCJA)** is a government, private, or public agency that provides services primarily for purposes other than the administration of criminal justice. Examples of noncriminal justice agencies that might access CJI include a 911 communications center that performs dispatching functions for a criminal justice agency (government), a bank needing access to criminal justice information for hiring purposes (private), or a county school board that uses criminal history record information to assist in employee hiring decisions (public).
- **Organizational Personnel with Information Security Responsibilities** are responsible for ensuring the confidentiality, integrity, and availability of CJI and the implementation of technology in compliance with the CJIS Security Policy.
  - **Local Agency Security Officer (LASO)** serves as the primary Information Security contact between a local law enforcement agency and the CSA. The LASO actively represents their agency in all matters pertaining to Information Security, including disseminating security alerts and maintaining security documentation.
  - **Authorized Recipient Security Officer (ARSO)** coordinates and oversees information security by ensuring that the approved fingerprint processing contractor adheres to the CJIS Security Policy, verifying the completion of Security and Privacy Training, and communicating with the FBI CJIS Division on matters relating to information security.

Agency Responsibilities

Agencies that access CJI are required to adhere to all technical and procedural requirements of the FBI CJIS Security Policy. They are also required to develop and publish internal information security policies, including penalties for misuse, and maintain a set of current written policies and procedures on how misuse of CJI will be handled.

Individual User Responsibilities

Individuals are responsible for maintaining their own conduct, as it pertains to CJI, and always practice responsible security behavior.

Individual user responsibilities include:

- Face computer monitors away from outside windows, doors, or hallways
- Limit access of CJI to completion of assigned duties
- Always accompany visitors to computer and workstation areas
- Do not use personally owned information systems to access, process, store, or transmit CJI (unless the agency has established and documented terms and conditions of such systems)
- Do not use public computers to access, process, store, or transmit CJI
- <u>**Never use CJI for personal use and gain**</u>

Top 5 Daily Security Rules

1. Use a unique user ID and password.
2. Be accountable for your actions while accessing and using CJI.
3. Do not share or leave passwords in conspicuous locations (keyboard, monitor, mousepad, or desk).
4. Use password protected screensavers and lock computer when stepping away from the desk. *Simply turning off the monitor during a break does not constitute a sufficient security precaution.*
5. Log out of the system at the end of your shift or when another operator wants to access the system.

What is CJI?

In the United States, the individual right to privacy is protected by the US Constitution. The Privacy Act of 1974 further protects personal privacy from misuse by regulating the **collection**, **maintenance**, **use**, and **dissemination** of information by criminal justice agencies.

Criminal Justice Information

Criminal Justice Information (**CJI**) is the term used to refer to all of the FBI Criminal Justice Information Services (CJIS) Division provided data necessary for law enforcement and civil agencies to perform their work.

CJI can include any of the following:

- **Fingerprints**
- **Personal data**
- **Property data**
- **Other information related to incidents and cases** (e.g., stolen cars, stolen guns, missing persons, etc.)

The National Crime Information Center (NCIC), located in West Virginia, is a computerized database of CJI available to law enforcement agencies nationwide. NCIC is supervised by the FBI CJIS Division, however the management of the information processed, stored, or transmitted to NCIC is a collaboration between the FBI and federal, state, local, and tribal criminal justice agencies.

Another important organization in the communication of criminal justice information is Nlets, a computer-based message switching system that connects every state, local, and federal law enforcement, justice, and public safety agency for the purposes of sharing and exchanging critical information.

Criminal History Record Information

All records in NCIC are protected from unauthorized access, however some records have additional restrictions due to the sensitive nature of the information.

Criminal History Record Information (CHRI) is arrest-based data collected by both national and state criminal justice agencies. CHRI is sometimes informally referred to as “restricted data” and is a subset of CJI.

CHRI data includes:

- Arrest descriptions and notations
- Other formal criminal charges
- Conviction status
- Sentencing data
- Incarceration or correctional supervision
- Probation and parole information

Interstate Identification Index

The **Interstate Identification Index (III)** is a “pointer” system that ties FBI criminal history files and state-level files maintained by each state into a national system. Federal, state, and local criminal justice agencies can use the III to conduct searches to determine whether an individual has a criminal record anywhere in the country. If so, that agency can then be pointed to the federal or state file from which the record may be obtained online.

The information obtained from the III is considered CHRI and should be accessed only for an authorized purpose. **All users must provide a reason for all III inquiries**.

NCIC Restricted Files

The restricted files, which should be protected as CHRI, are as follows:

- Gang Files
- Threat Screening Center Files
- Supervised Release Files
- National Sex Offender Registry Files
- Historical Protection Order Files
- Identity Theft Files
- Protective Interest Files
- Person With Information (PWI) data in Missing Persons Files
- Violent Person File
- National Instant Criminal Background Check System (NICS) Denied Transaction

NCIC Non-Restricted Files

All NCIC files which cannot be classified as CHRI or as an NCIC Restricted File are considered **NCIC Non-Restricted Files**.

Personally Identifiable Information

Personally Identifiable Information (PII) is information which can be used to distinguish or trace an individual’s identity. Any FBI CJIS provided data maintained by an agency, including education, financial transactions, medical history, and criminal or employment history may include PII.

Examples of PII include:

- Name
- Social security number
- Biometric records (such as fingerprints, retina scans, facial geometry)
- Driver’s License or Passport number
- Personal address information (including physical or email addresses)

Other personal or identifying information, such as date of birth, place of birth, mother’s maiden name, gender, or race, are not technically PII because more than one person could share these traits. However, when combined with PII, they could be used to identify a specific individual and are therefore protected.

Agencies must develop policies, based on state and local privacy rules, to ensure appropriate controls are applied when handling PII extracted from CJI.

Proper Access, Use, & Dissemination of CJI

Note: This section applies to the access, use, and dissemination of Criminal History Record Information (CHRI), NCIC Restricted Files Information, NCIC Non-Restricted Files Information, and NCIC Non-Restricted Files Information Penalties.

The FBI Security Policy provides the minimum standard for the proper access, use, and dissemination of CJI, however local policies may **increase** restrictions.

Information Handling

CJI is sensitive, so special consideration regarding the purpose and usage of CJI and CHRI should be made at all times to prevent unauthorized or improper access, use, dissemination, and release.

Authorized Purposes

Access to and use of CJI and CHRI is primarily for criminal justice purposes, however access can be granted for the performance of a noncriminal justice function in certain circumstances, as authorized by federal or state law.

Authorized **criminal justice purposes** include criminal identification and the collection, storage, and dissemination of criminal history record information. Types of criminal identification are:

- Detection
- Apprehension
- Pre-trial release
- Post-trial release
- Prosecution
- Adjudication
- Detention
- Correctional supervision
- Rehabilitation of accused persons or criminal offenders

Authorized **noncriminal justice purposes** for using criminal history records may include:

- Employment suitability
- Licensing determinations
- Immigration and naturalization matters
- National security clearances

CJI should never be queried for personal benefit.

Authorized Usage

Once CHRI has been obtained from the III system it must be used for the **same** authorized purpose for which it was requested.

EXAMPLE:

John Doe is hired to perform some plumbing work at a local police department. The department runs a III check using purpose code C for site security. One month later, he applies for an employment position at the same local police department. Rather than use the information from the previous search, a new III check must be performed with purpose code J for employment suitability.

Note: These are only example codes. Please refer to your agency's policy for your authorized purpose codes.

CJI Dissemination

CJI is distributed only as a part of the user's criminal justice duties on a need-to-know, right-to-know basis. Special consideration should be made at all times to protect CJI from improper disclosure.

Sharing information or using information for anything other than job-related criminal justice duties constitutes a violation of user privileges. CJI should never be shared with friends, relatives, or anyone who does not require the information for their official duties.

Phone/Radio

Voice transmission of a criminal history should be limited, and details should only be given over a radio or cell phone when an officer determines that there is an immediate need for the CJI to further an investigation or in situations affecting the safety of an officer or the general public.

Email

Email may be a compliant method to disseminate CJI provided that the email client/server, application, or service meets the encryption and authentication requirements. Additionally, appropriate spam and antivirus protections must be in place.

Always verify the recipient's authorization ***before*** sending CJI in an email.

Faxing

An agency may use a facsimile (fax) machine to send CJI, provided that both the sending and receiving agencies have an Originating Agency Identifier (ORI) and are authorized to receive CJI. The encryption requirements for CJI in transit must be used unless the fax is being sent over a standard telephone line.

Always verify the receiving agency's authenticity ***before*** sending a fax transmission.

Chat/Text

Texting using cellular service provider SMS or MMS functions should not be considered secure or appropriate for transmission of CJI data. Chat or Texting applications which authenticate using embedded passwords or device identifier only should not be considered secure.

Only third-party applications utilizing appropriate encryption and authentication methods independent of the device password/PIN may provide a compliant solution.

Media Protection

Media Access

Access to all digital and non-digital media should be restricted to authorized individuals.

Digital Media

An example of restricting access to digital media would be to limit access to design specifications on a flash drive to the system development team.

Examples of digital (i.e., electronic) media include:

- Diskettes
- Magnetic tapes
- CDs/DVDs
- External or removable hard drives
- USB flash drives

Non-digital Media

An example of restricting access to non-digital media would be to deny access to hard copies of case file information stored in a locked filing cabinet.

Examples of non-digital (i.e., physical) media include:

- Paper
- Microfilm
- Fax ribbon

Media Storage

Digital and non-digital media should be securely stored and physically controlled within a physically secure location or controlled area. Encryption of CJI on digital media should be employed when physical and personnel restrictions are not feasible.

Secure storage of media includes:

- Locked drawer, desk, or cabinet
- Controlled media library

Physically controlling stored media includes:

- Conducting inventories
- Ensuring procedures are in place to allow users to check out and return media
- Maintaining accountability for stored media

Media Disposal

Formal procedures for the secure disposal of physical media should minimize the risk of compromising sensitive information. Proper disposal or destruction should be witnessed or carried out by authorized personnel.

Electronic Media Disposal

- Electronic media must be sanitized prior to disposal (before reusing or transferring to a non-criminal justice entity).
- Physical destruction is recommended for disposal of electronic media.
- If physical destruction is not possible, it must be overwritten <u>at least three times</u> or more to prevent unauthorized access to previously stored data.

Physical Media Disposal

- The two most popular methods for destruction of physical media (hard copies) are:
  - Shredding
  - Incineration

Access, Use, & Dissemination Penalties

Unauthorized **requests**, **receipt**, **release**, **interception**, **dissemination**, or **discussion** of CJI is serious and may result in the following:

- <u>Criminal prosecution</u>
- <u>Termination of employment</u>

Personnel Sanctions

Agencies must have a formal sanctions process for personnel failing to comply with established information security policies and procedures.

The agency will perform a formal disciplinary process for any personnel who fail to comply with the security policies and procedures. Continued misuse of CJI could result in an agency being denied access until the violations have been corrected.

Access Control

Access control provides the planning and implementation of mechanisms to restrict the reading, writing, processing, and transmission of CJIS information. It also provides restrictions for the modification of systems, applications, services, and communication configurations allowing access to CJIS information.

Access Control Criteria

Agencies should control access to CJI based on one or more of the following:

- Job assignment or function of the user seeking access
- Physical location
- Logical location
- Network addresses (e.g., users from sites *within* a given agency may be permitted greater access than those from outside the agency)

- Time-of-day and day-of-week/month restrictions

Access Control Mechanisms

When setting up access controls, agencies should use one or more of the following mechanisms:

- **Access Control Lists (ACLs)** are a register of users (including groups, machines, processes) who have been given permission to use a particular system resource and the types of access they have been permitted.
- **Resource Restrictions** are where users are never allowed to request information, functions, or other resources for which they do not have access. Three major types of resource restrictions are: menus, database views, and network devices.
- **Encryption** is where encrypted information can only be decrypted and read by those possessing the appropriate cryptographic key.
- **Application Level** is where security is employed at the application level (in addition to system level security).

Access Enforcement

It is recommended that agencies enforce access to CJI by implementing two important security principles: least privilege and separation of duties.

Least Privilege

The security principle of **least privilege** is where individuals are granted only the most restrictive set of access privileges required to perform their official duties. This limits access to CJI to only authorized personnel with the need and the right to know.

Logs of access privilege changes shall be maintained for a minimum of ***one year*** or equal to the agency's record retention policy–whichever is greater.

Separation of Duties

The security principle of **separation of duties** is the division of roles and responsibilities so that different individuals perform each function related to administrative duties. For example, those with the ability to create and assign user access to the system should not be able to access the audit logs that contain the evidence of the account actions.

Personnel Access

Having proper personnel security measures against the insider threat is a critical component of information security.

Screening Requirements

All personnel, including contractors and vendors, must be screened prior to being granted access to CJI.

The following are the minimum requirements for screening individuals needing access to CJI:

- All personnel who will have unescorted access to unencrypted CJI must be screened ***prior*** to being granted access to CJI (including contractors and vendors)
- Screening must include state of residency and national fingerprint-based records checks
- All requests for access must be made as specified by the CSO, and only the CSO or their designee (from an authorized criminal justice agency) may approve access to CJI
- If a record <u>of any kind</u> exists, access to CJI will not be granted until the CSO or their designee reviews the matter to determine if access is appropriate
- The granting agency must maintain a list of personnel who have authorized access to CJI
- It is recommended that individual background re-investigations be conducted ***every five years***

Checks are not necessary if the individual is always escorted by authorized personnel.

Transfer

CJI access authorizations must be reviewed when personnel are reassigned or transferred to other positions within the agency. If changes need to be made, all appropriate actions must be taken such as closing and establishing accounts and modifying system access authorizations.

Termination

Upon termination of personnel, the agency must immediately discontinue access to any local agency systems which can access CJI. If the employee is an employee of a Non-Criminal Justice Agency or a Contractor, the employer must notify all agencies that may be affected by the personnel change.

Contractor/Vendor Access

Private contractors who perform criminal justice functions must meet the same training and certification criteria required by governmental agencies performing a similar function. They are also subject to the same audit review as a local agency.

CJIS Security Addendum

All private contractors who perform criminal justice functions must sign the **CJIS Security Addendum**, an addendum to the agreement between a criminal justice agency and a private contractor.

The Security Addendum includes security provisions for contractors:

- Authorizes access to CJI
- Limits the use of the information for the purposes for which it is provided
- Ensures the security and confidentiality of the information consistent with existing regulations
- Provides for sanctions
- Other provisions as the Attorney General may require

This security addendum shall be incorporated in the agreement that specifies the contractor's scope and purpose for providing services.

Physical Security

The areas that process or store Criminal Justice Information (CJI) should be physically secure to prevent unauthorized access.

Physical Access Authorizations

To ensure physical security, agencies are responsible for:

- Developing and maintaining a current list and issuing credentials to personnel with authorized access to the physically secure location
- Prominently posting the perimeter of the area requiring physical security and separating it from nonsecure locations by physical controls

Physical Access Control

All access points to a physically secure location must be controlled, and individual access authorizations should be verified before granting access.

Physical Controls

The physical controls required in order to be considered a physically secure location are:

Monitoring Physical Access

Agencies should monitor physical access to the information system to detect and respond to physical security incidents.

Access Control for Transmission Medium

Agencies should control physical access to information system distribution and transmission lines within the physically secure location.

Access Control for Display Medium

Agencies must position information system devices in such a way as to prevent unauthorized individuals from accessing and viewing CJI.

Delivery and Removal

Agencies must authorize and control information system-related items entering and exiting the physically secure location.

Visitor Control

Agencies should control physical access by authenticating visitors before authorizing escorted access to the physically secure location (except for those areas designated as publicly accessible). The agency shall escort visitors at all times and monitor visitor activity within the physically secure location.

Controlled Areas

If an agency cannot meet all of the controls required for establishing a physically secure location but has an operational need to access or store CJI, the agency shall designate an area, room, or storage container as a controlled area for the purpose of day-to-day CJI access or storage.

This controlled area should have the following security measures:

- Store hard copies containing CJI in such a manner as to prevent unauthorized or inadvertent access
- Follow the encryption requirements in the CJIS Security Policy for CJI data at rest
- Position information system devices and documents containing CJI in such a way as to prevent unauthorized individuals from access and view
- Limit access to the area *only* to those personnel authorized by the agency to access or view CJI
- Lock the area, room, or storage container when unattended

It is the responsibility of *all personnel* to help ensure that these areas stay secure. You are encouraged to be mindful of the physical security at all times.

System Security

System Security, or IT Security, is hardware or software used to assure the integrity and protection of information and the means of processing it.

System Access Control

Access control mechanisms to enable systems access to CJI should be restricted by object (e.g., data set, volumes, files, records), including the ability to read, write, or delete the objects.

Access controls must be in place and operational for all information systems to:

- Prevent multiple simultaneous active sessions for the same User ID in applications accessing CJI
- Ensure that only authorized personnel can add, change, or remove component devices, dialup connections, and remove or alter programs

System Use Notification

Before granting access, the information system should display an approved system use notification message informing potential users of various usages and monitoring rules.

The system use notification message must, at a minimum, provide the following information:

- 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

Session Lock

To prevent unauthorized access to the system, an automatic session lock, such as a **screensaver with a password**, must be initiated after a maximum of ***30 minutes*** of inactivity.

Note: A session lock is not a substitute for logging out of the information system.

For safety reasons, the following may be exempt from this requirement:

- Devices that are part of any enclosed mobile vehicle used for the purposes of criminal justice activities
- Devices that are used to perform dispatch functions and located within a physically secure location
- Terminals designated solely for the purpose of receiving alert notifications (i.e., receive only terminals [ROT]) used within a physically secure location facilities that remain staffed when in operation

Identification and Authentication

Each organizational user who is authorized to store, process, or transmit CJI, including individuals considered to have an equivalent status to employees (e.g., contractors and guest researchers), must be uniquely identified and authenticated.

Identification

Identification is a unique, auditable representation of an identity within an information system usually in the form of a simple character string for each individual user, machine, software component, or any other entity.

Examples of Identifiers include:

- Personal Identifier (i.e., User ID)
- Agency Identifier (i.e., ORI)
  Note: The FBI authorized originating agency identifier (ORI) must be used in each transaction on CJIS systems.
- Device Identifier (e.g., Media Access Control [MAC] addresses, Internet Protocol [IP] addresses, device-unique tokens)

Identifiers that have been previously used by an individual, group, role, service, or device may not be assigned to a different individuals, groups, roles, services, or devices for at least ***one year***.

Authentication

Authentication refers to mechanisms or processes to verify the identity of a user, process, or device, as a prerequisite to allowing access to a system's resources. Software or systems approved to access CJI—whether provided by the State/Federal agency, developed by a local agency, or purchased from a vendor—must follow the authentication requirements defined in the FBI CJIS Security Policy.

Multi-Factor Authentication

Multi-factor authentication requires the use of two or more *different* factors to achieve authentication. Authentication factors include something you know, something you have, or something you are (e.g., a biometric). Verifying multiple factors provides a higher level of confidence that the requester possesses and controls the authenticators tied to the subscriber's account.

There are five main types of authenticators that can be used in multi-factor authentication:

- **Memorized Secrets –** a secret value intended to be chosen and memorized by the user (e.g., passwords, passphrases, PINs); *something you know*
- **Look-up Secrets –** physical or electronic record that stores a set of secrets shared between the requester and the organization (e.g., bingo cards, recovery keys); *something you have*
- **Out-of-Band Devices –** a physical device that is uniquely addressable and can communicate securely with the verifier over a secondary channel (e.g., receiving a 6-digit code on your mobile device); *something you have*
- **OTP Authenticators –** One-time Password (OTP) is generated by a device for authentication (e.g., an authenticator app on your mobile device generates a 6-digit code every sixty seconds); *something you have*
- **Cryptographic Authenticators –** a cryptographic key stored on a disk or some other "soft" media (e.g., physical tokens, smartcards); *something you have*

Note: Some OTP and cryptographic authenticators require an additional authentication factor to activate, such as an integral entry pad or biometric (e.g., fingerprint) reader, or a direct computer interface (e.g., USB port).

If the multi-factor authentication process uses a combination of two single-factor authenticators, then it must include a Memorized Secret authenticator and a possession-based authenticator (i.e., something you have).

<u>All systems with direct access to CJI must utilize multi-factor authentication.</u> Direct access means an authorized user would have the ability to query a state or national criminal record repository.

Memorized Secret Requirements

Note: For a full list of memorized secret requirements, see IA-5(1)(a) in the CJIS Security Policy.

If basic password standards are being followed, memorized secrets must:

- Be a minimum of 8 characters
- Be changed at least every ***90 calendar days***
- Not be the same as the User ID
- Not be a proper name
- Not be a dictionary word
- Not be identical to the previous 10 passwords
- Not be displayed when entered
- Not be transmitted outside of the secure domain

Password Examples (following basic standards):

BAD Password	Reason	BETTER Password
5kidz	Too short	F!v3Kidz
Elephant	Dictionary word	El3ph@nt!
Alexandria	Proper Name	@L3xndr1a

System and Communications Protection

System and communications protection helps safeguard the flow of information within an information system through boundary and transmission protection.

Encryption

Encryption is the process of converting information or data into a code to prevent unauthorized access. **Decryption** is the process of converting the information back from its encrypted state into a plaintext (readable) format.

There are two main types of encryption: symmetric encryption and asymmetric encryption (also known as public key encryption).

System and Information Integrity

System and information integrity helps ensure that the information being accessed has not been tampered with or damaged by an error in the information system.

Malicious Code Protection

Malicious code, also known as **malware**, refers to a program that is covertly inserted into another program with the intent to compromise the confidentiality, integrity, or availability of the data, application, or operating system.

To protect against malicious code, agencies should:

- For all systems with internet access: implement malicious code protection that includes automatic updates
- For all systems *not* connected to the internet: implement local procedures to ensure malicious code protection is kept current
- Employ virus protection mechanisms to detect and eradicate malware (e.g., viruses, worms, Trojan horses) at critical points throughout the network and on all workstations, servers and mobile computing devices on the network
- Ensure malicious code protection is enabled on all of the aforementioned critical points and information systems and that resident scanning is used

Spam and Spyware Protection

Spam and spyware protection must be implemented on all organizational email systems, removable media (e.g., USB memory sticks, external hard drives, etc.), and all internet access points.

Spam and spyware protection includes:

- Spam protection mechanisms at critical information system entry points (e.g., firewalls, electronic mail servers, remote-access servers)
- Spyware protection at workstations, servers, and mobile computing devices on the network
- Spam and spyware protection mechanisms designed to detect and take appropriate action on unsolicited messages and spyware/adware

Handheld Device Security

Handheld, or mobile, devices have both physical and wireless security issues. Organizations must be aware of potential threats on both fronts and ensure that these devices meet the following minimum requirements to avoid them. Mobile devices include pagers, cell phones, personal digital assistants (PDAs), laptops, or other portable devices.

Cellular Devices

A cellular device is any device that is capable of employing cellular technology, including smartphones (i.e., Blackberry, iPhones, etc.), tablets, and PDAs. Threats to cellular handheld devices stem mainly from their size, portability, and available wireless interfaces and associated services.

Examples of threats to cellular handheld devices include:

- Loss, theft, or disposal
- Unauthorized access
- Malware
- Spam
- Electronic eavesdropping
- Electronic tracking
- Cloning

Bluetooth

Bluetooth technology has been integrated into many types of business and consumer devices, including cell phones, laptops, automobiles, medical devices, printers, keyboards, mice, headsets, and biometric capture devices. Bluetooth technology is susceptible to general wireless networking threats (e.g., denial of service attacks, eavesdropping, man-in-the-middle attacks, and message modification) as well as attacks that target known vulnerabilities in Bluetooth implementations and specifications.

Organizational security policy should be used to dictate the use of Bluetooth and its associated devices based on the agency’s operational and business processes.

Mobile Device Management (MDM)

Mobile Device Management (MDM) allows for the implementation of security controls for mobile devices and the centralized oversight of configuration control, application usage, and device protection and recovery.

The following controls should be implemented when directly accessing CJI from devices running a limited-feature operating system:

- Ensure that CJI is only transferred between CJI authorized applications and storage areas of the device
- MDM with at least the following controls:
    - Remote locking of device
    - Remote wiping of device
    - Setting and locking device configuration
    - Detection of “rooted” and “jailbroken” devices
    - Enforcement of folder or disk level encryption
    - Application of mandatory policy settings on the device
    - Detection of unauthorized configurations
    - Detection of unauthorized software or applications
    - Ability to determine the location of agency-controlled devices
    - Prevention of unpatched devices from accessing CJI or CJI systems
    - Automatic device wiping after a specified number of failed access attempts

Devices that have had any unauthorized changes made to them, such as being rooted or jailbroken, should not be used to process, store, or transmit CJI data at any time.

Wireless Device Risk Mitigations

To reduce the risks associated with wireless devices, the following practices should be employed:

- Use multi-factor authentication
- Encrypt all CJI on the device
- Employ personal firewalls
- Employ anti-virus software
- Configure for local device authentication
- Erase cached information when session is terminated
- Apply available critical patches and upgrades to the operating system

Wireless Device Malicious Code Protection

Appropriately configured MDM software is capable of checking the installed applications on the device and reporting the software inventory in a similar manner to traditional virus scan detection of unauthorized software. This provides a high degree of confidence that only known software or applications are installed on the device. Any device natively capable of performing these functions without an MDM solution is acceptable.

Agencies that allow smartphones and tablets to access CJI should have an approval process for the use of specific software or applications on the devices.

Remote Access

Remote access is any temporary access to an agency's information system by a user through an external, non-agency-controlled network.

All remote access must be controlled by the agency through managed access control points. Remote Access may be permitted for privileged functions *only for compelling operational needs*. Documentation on the technical and administrative process for enabling remote access must be included in the security plan for the information system.

Personally Owned Information Systems

Personally owned information systems should **not** be used to access, process, store, or transmit CJI unless the agency has established and documented the specific terms and conditions for personally owned information system usage.

If personally owned mobile devices are used as part of a Bring Your Own device (BYOD) program, special handling procedures and processes may need to be developed to ensure those devices are compliant. Keep in mind that the technical methods and risk to achieve compliance with BYOD devices may exceed any cost savings potentially achieved through the program.

Publicly Accessible Computers

Publicly accessible computers should **not** be used to access, process, store, or transmit CJI.

Examples of publicly accessible computers include (but not limited to):

- Hotel business center computers
- Convention center computers
- Public library computers
- Public kiosk computers

Audit Monitoring, Analysis, & Reporting

Agencies must designate an individual or position to perform the following audit monitoring, analysis, and reporting activities:

- Review/analyze information system audit records for indications of inappropriate or unusual activity
- Investigate suspicious activity or suspected violations
- Report findings to appropriate officials
- Take necessary actions

Audit review/analysis should be conducted at a minimum ***once a week***. The frequency of review/analysis should be increased to match the increased volume of an agency's processing or whenever there is an indication of higher risk to agency operations, agency assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

Incident Response

Security Incidents

A **security incident** is a violation of the CJIS Security Policy that threatens the confidentiality, integrity, or availability of CJI.

Incident Indicators

Security incidents are not always obvious. In some cases, you may only see *indicators* of an incident. Examples of indicators include:

- New user accounts are mysteriously created which bypass standard procedures
- Sudden high activity on an account that has had little or no activity for months
- Accounting discrepancies
- Data modification or deletion
- Changes in file lengths or modification dates
- New files with novel or strange names appear
- Attempts to write to system files
- Unexplained poor system performance
- The system unexpectedly crashes without clear reasons
- Denial of service
- Suspicious probes
- Suspicious browsing

Security Incident Policy

Each agency accessing CJI must establish a written policy describing the overall incident handling procedures, how the agency performs incident reporting, and incident management procedures in the event of a security incident.

Authorized users who have direct access to CJI and all appropriate IT personnel should be aware of the agency's policy regarding possible security incidents and the proper reporting procedures within the agency.

Incident Response Training

Agencies must ensure that general incident response roles and responsibilities are included as part of required security and privacy training.

Incident Handling

There are four phases in the incident response life cycle which will assist in the handling of a security incident:

Preparation

Preparation involves establishing and training an incident response team and acquiring the necessary tools and resources to manage an incident.

Detection and Analysis

Detection and analysis begin when a security incident has occurred. The method of attack, as well as the impact to the systems and personnel involved must be determined.

Containment, Eradication, & Recovery

Containment activities for computer security incidents involve decision-making and the application of strategies to help control attacks and damage, cease attack activities, or reduce the impact or damage caused by the incident.

Eradication efforts for a computer security incident involve removal of the security threat, including removal of latent threats (e.g., malware, invalid user accounts, etc.) and identification of any vulnerabilities caused by the incident.

Recovery efforts for incidents involve restoration of affected systems to normal operation.

Post-Incident Activity

Post-incident activities involve the reflection, compilation, and analysis of the activities that occurred leading to the security incident, and the actions taken by those involved in the security incident.

Agencies should incorporate the lessons learned from ongoing incident handling activities into the incident response procedures. Wherever possible, the incident handling process should be automated.

Reporting Security Events

Report any incidents or unusual activity to your agency contact, Local Agency Security Officer (LASO), or Information Security Officer (ISO) ***immediately***.

All personnel are required to report any suspected incident, regardless of how minor it might seem.

Security Incident Report

It is important that you include the following information in your report of the incident:

- Date of Incident
- Location of Incident
- Systems Affected
- Method of Detection
- Description of Incident
- Actions Taken/Resolution
- Date & Contact Info for Agency

Conclusion

Thank you for reviewing the Security and Privacy Training! As a reminder, this training must be completed ***every year*** to remain compliant with the FBI CJIS Security Policy.

Questions

If you have any questions regarding the CJIS Security Policy or the expected behavior around Criminal Justice Information (CJI), talk to your Agency Contact or Local Agency Security Officer (LASO) for further information.

Next Steps

Depending on your organization’s requirements, there may be additional training and/or a test to complete your certification.

Limited Access v8.2024.1

1. Limited Access V4

1.1 Home Page

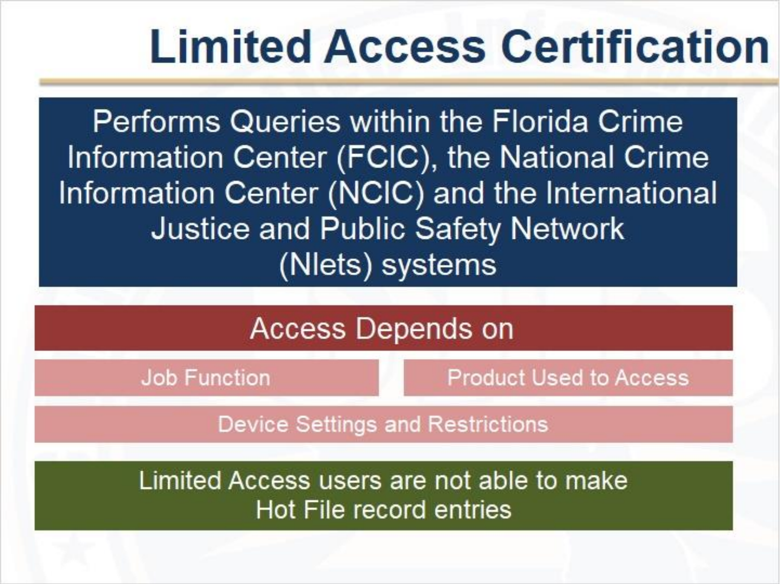
Limited Access Certification

Criminal Justice Information Services
CJIS
Florida Department of Law Enforcement

Notes:

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

1.2 Introduction



Limited Access Certification

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

Access Depends on

Job Function

Product Used to Access

Device Settings and Restrictions

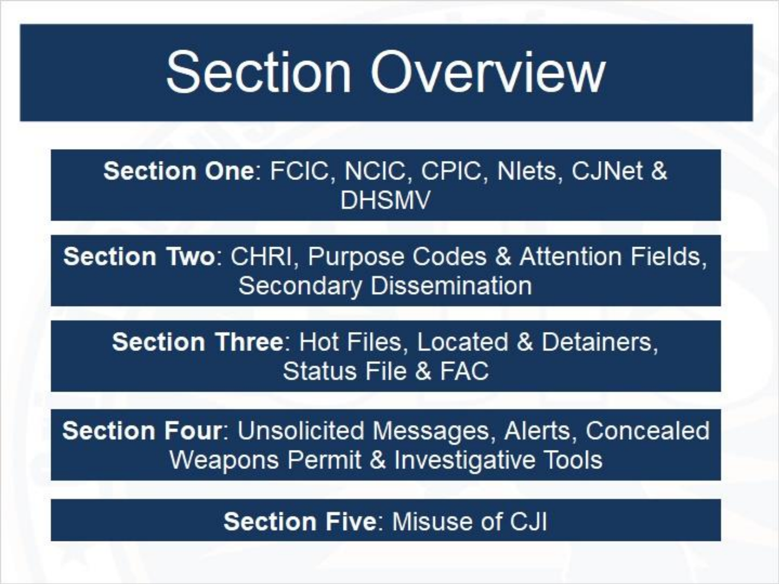
Limited Access users are not able to make Hot File record entries

Notes:

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

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

1.3 Section Overview



Section Overview

Section One: FCIC, NCIC, CPIC, Nlets, CJNet & DHSMV

Section Two: CHRI, Purpose Codes & Attention Fields, Secondary Dissemination

Section Three: Hot Files, Located & Detainers, Status File & FAC

Section Four: Unsolicited Messages, Alerts, Concealed Weapons Permit & Investigative Tools

Section Five: Misuse of CJI

Notes:

The Limited Access Certification training is comprised of five sections.

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

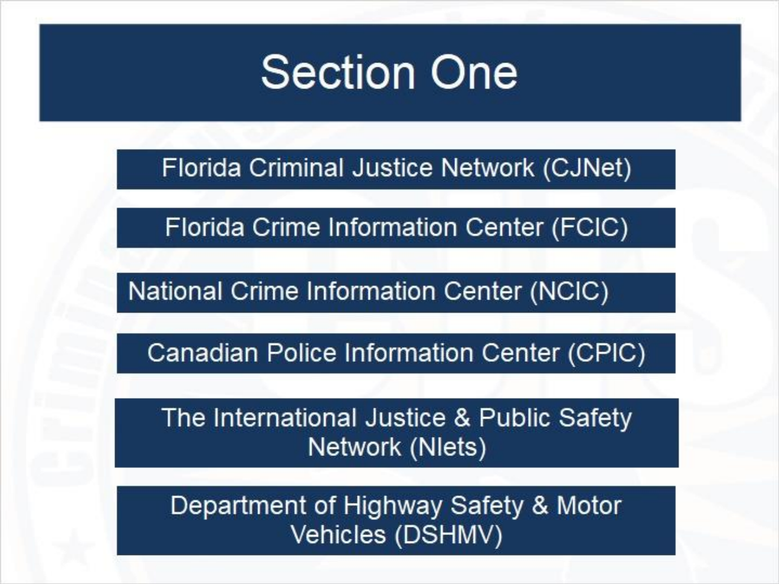
-Section Two will highlight Criminal History Record Information (CHRI), Purpose Codes, Attention Fields, and the use and purpose of the Secondary Dissemination Log;

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

-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 and;

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

1.4 Section One



Section One

Florida Criminal Justice Network (CJNet)

Florida Crime Information Center (FCIC)

National Crime Information Center (NCIC)

Canadian Police Information Center (CPIC)

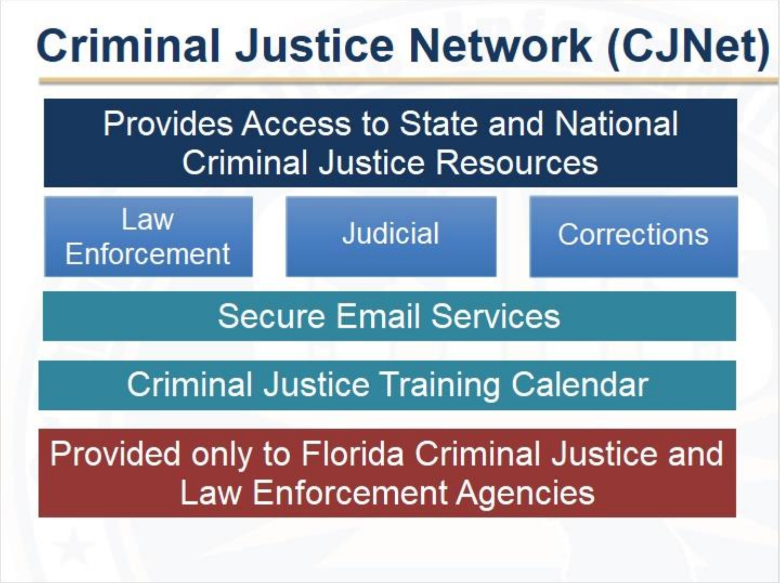
The International Justice & Public Safety Network (Nlets)

Department of Highway Safety & Motor Vehicles (DSHMV)

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 the FCIC, NCIC, CPIC and the International Justice and Public Safety Network, or Nlets, and the departments that maintain and provide access to these databases. Lastly, information on the various FCIC records that are provided by the Florida Department of Highway Safety and Motor Vehicles will be discussed.

1.5 Criminal Justice Network (CJNet)



Criminal Justice Network (CJNet)

Provides Access to State and National Criminal Justice Resources

Law Enforcement

Judicial

Corrections

Secure Email Services

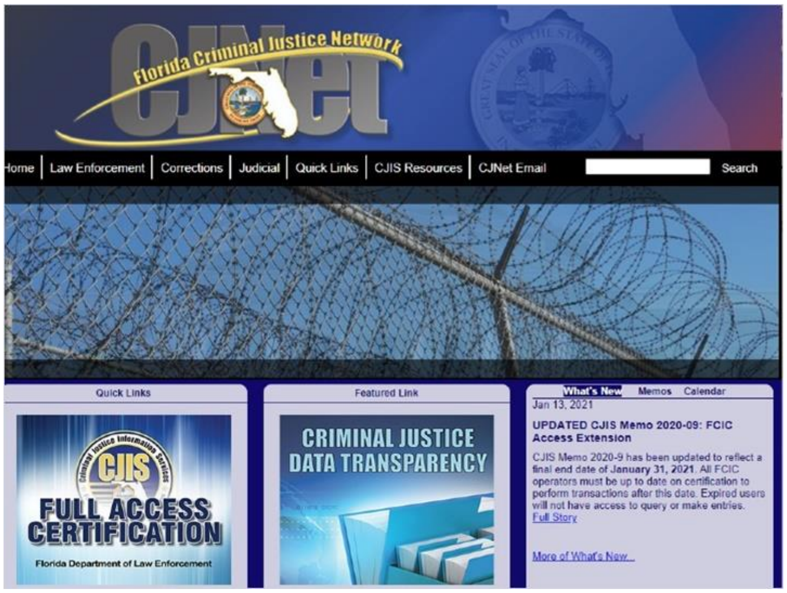
Criminal Justice Training Calendar

Provided only to Florida Criminal Justice and Law Enforcement Agencies

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. Users may access secure email services provided on the CJNet by using a web browser to access https://mail.flcjn.net. Users must ensure the “s” follows the http in the web address. From this secure web address, users may send an encrypted email from one CJNet user account to another CJNet user account”. Users must not send sensitive information containing CJI from a CJNet email account to an external non-CJNet email account. CJNet also has 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


Florida Criminal Justice Network
CJNet
Home
Law Enforcement
Corrections
Judicial
Quick Links
CJIS Resources
CJNet Email
Search
Quick Links
Criminal Justice Information Services
CJIS
FULL ACCESS CERTIFICATION
Florida Department of Law Enforcement
Featured Link
CRIMINAL JUSTICE DATA TRANSPARENCY
What's New
Memos
Calendar

Jan 13, 2021

UPDATED CJIS Memo 2020-09: FCIC Access Extension

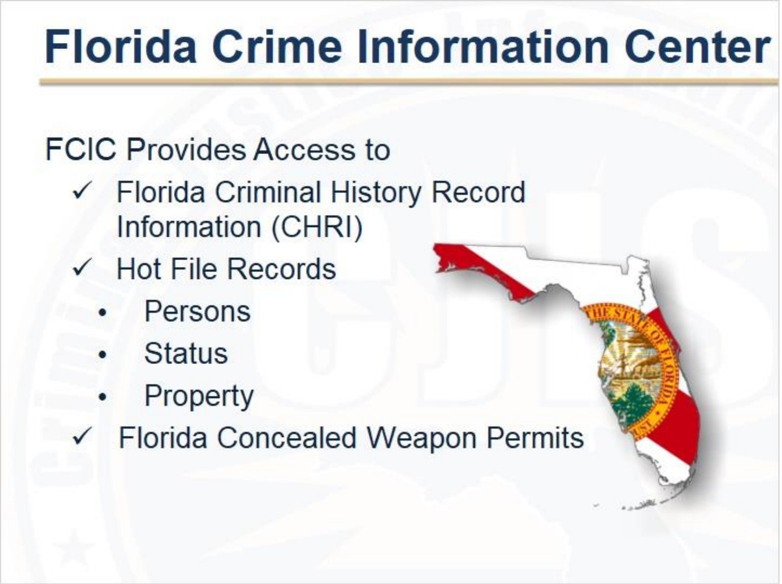
CJIS Memo 2020-9 has been updated to reflect a final end date of **January 31, 2021**. All FCIC operators must be up to date on certification to perform transactions after this date. Expired users will not have access to query or make entries.
Full Story

More of What's New...

Notes:

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

1.7 Florida Crime Information Center (FCIC)



Florida Crime Information Center

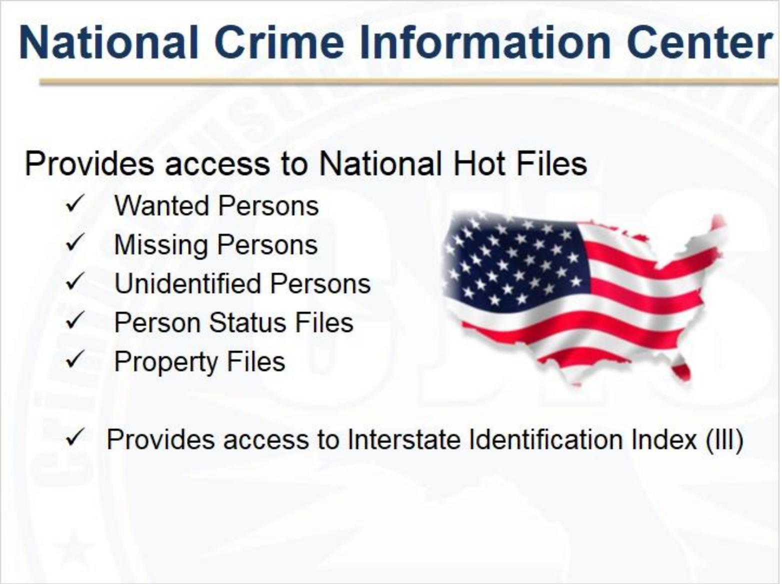
FCIC Provides Access to

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

Notes:

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

1.8 National Crime Information Center (NCIC)



National Crime Information Center

Provides access to National Hot Files

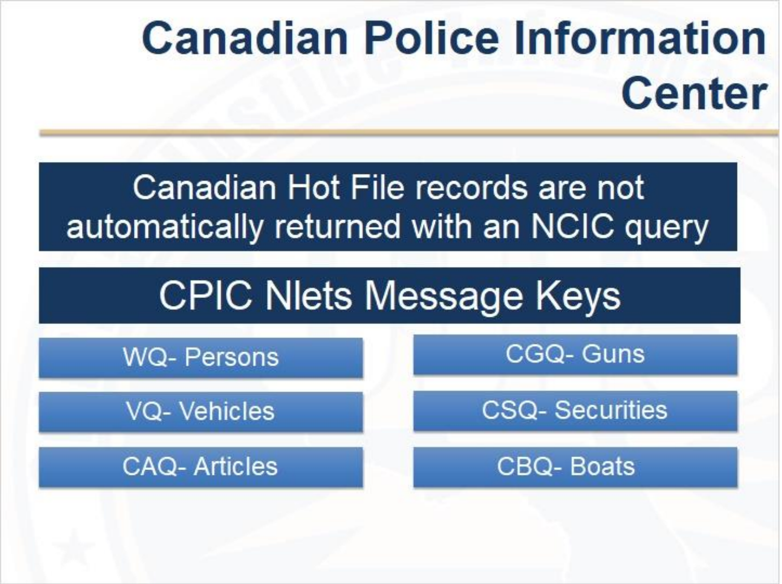
- ✓ Wanted Persons
- ✓ Missing Persons
- ✓ Unidentified Persons
- ✓ Person Status Files
- ✓ Property Files

- ✓ Provides access to Interstate Identification Index (III)

Notes:

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

1.9 CPIC



Canadian Police Information Center

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

CPIC Nlets Message Keys

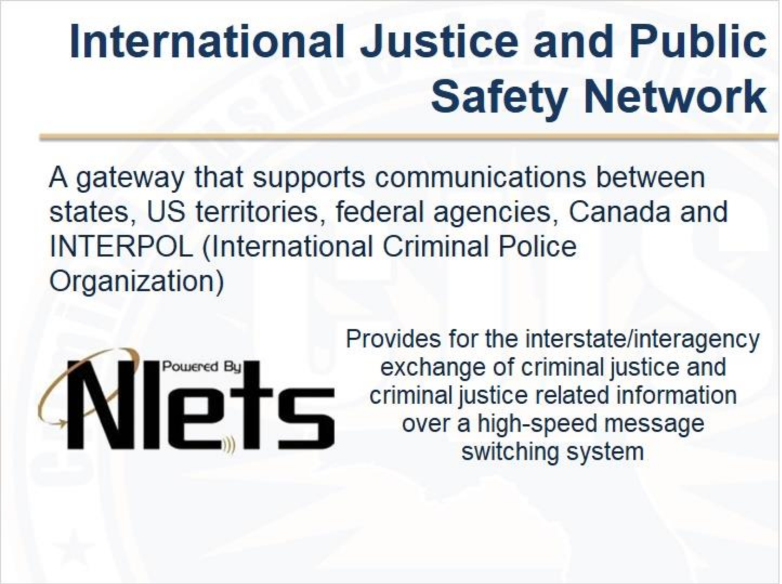
WQ- Persons	CGQ- Guns
VQ- Vehicles	CSQ- Securities
CAQ- Articles	CBQ- Boats

Notes:

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

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

1.10 International Justice and Public Safety Network (Nlets)



International Justice and Public Safety Network

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

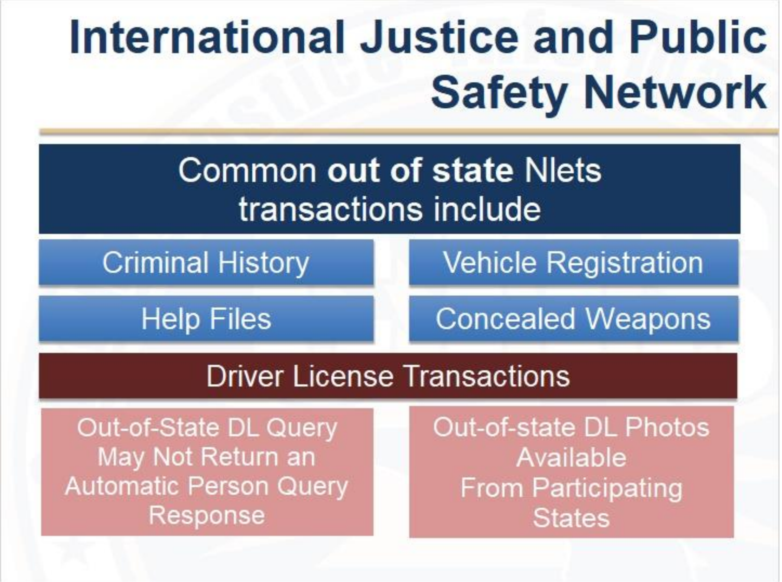
Powered By
Nlets

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

Notes:

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

1.11 Nlets



International Justice and Public Safety Network

Common **out of state** Nlets transactions include

Criminal History

Vehicle Registration

Help Files

Concealed Weapons

Driver License Transactions

Out-of-State DL Query May Not Return an Automatic Person Query Response

Out-of-state DL Photos Available From Participating States

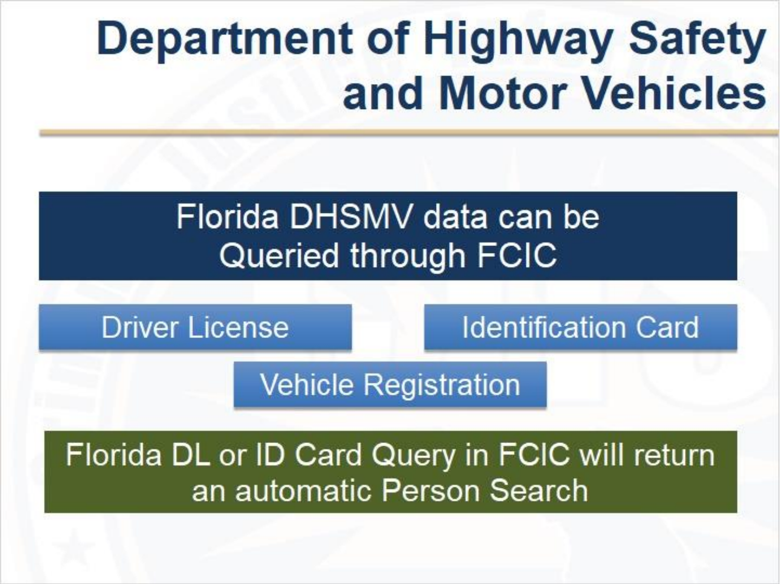
Notes:

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

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

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

1.12 DHSMV



Department of Highway Safety and Motor Vehicles

Florida DHSMV data can be Queried through FCIC

Driver License

Identification Card

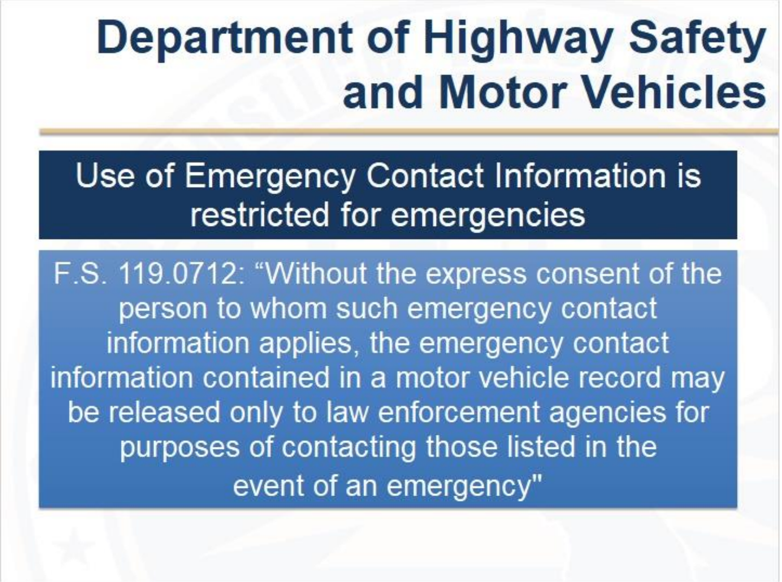
Vehicle Registration

Florida DL or ID Card Query in FCIC will return an automatic Person Search

Notes:

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

1.13 DHSMV



Department of Highway Safety and Motor Vehicles

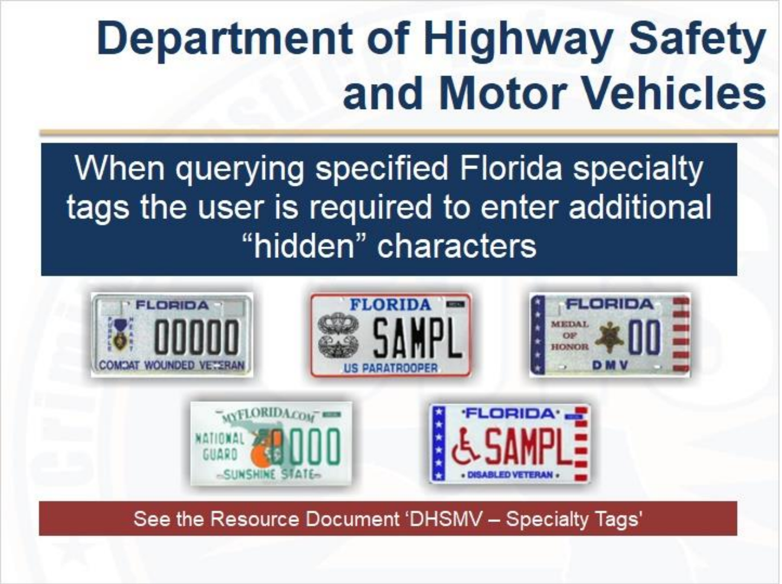
Use of Emergency Contact Information is restricted for emergencies

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

Notes:

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

1.14 DHSMV



Department of Highway Safety and Motor Vehicles

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

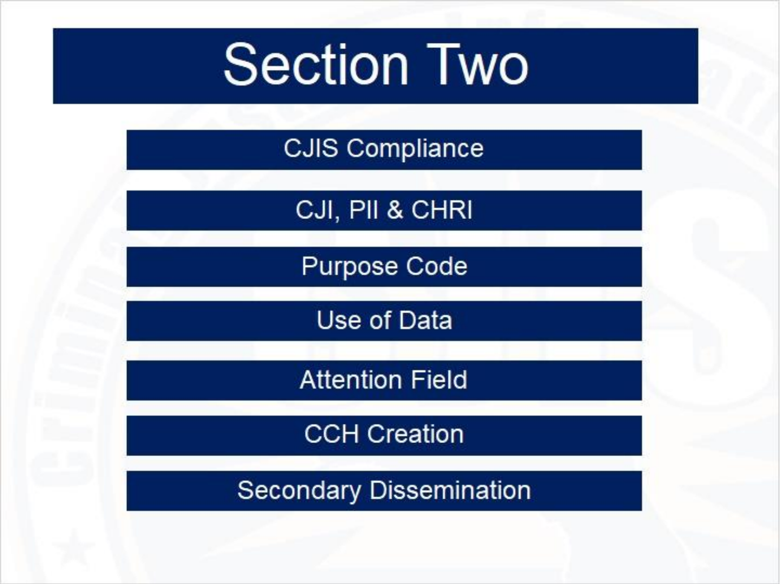
FLORIDA
00000
COMBAT WOUNDED VETERAN
FLORIDA
SAMPL
US PARATROOPER
FLORIDA
MEDAL OF HONOR
00
DMV
MYFLORIDA.COM
NATIONAL GUARD
0000
SUNSHINE STATE
FLORIDA
SAMPL
DISABLED VETERAN

See the Resource Document ‘DHSMV – Specialty Tags'

Notes:

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

1.15 Section Two



Section Two

CJIS Compliance

CJI, PII & CHRI

Purpose Code

Use of Data

Attention Field

CCH Creation

Secondary Dissemination

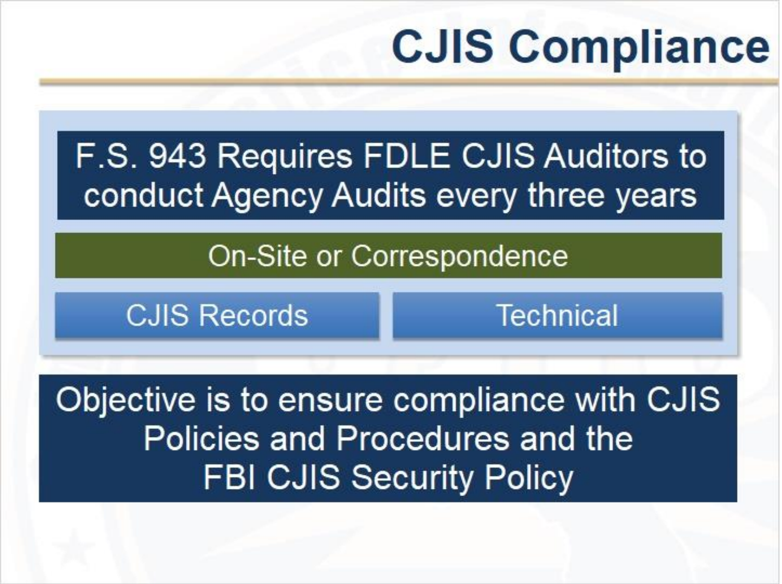
Notes:

Section Two of the Limited Access Certification Course provides an overview of several topics. The first topic is Criminal Justice Information Services (CJIS) Compliance, Criminal Justice Information (CJI), Personal Identifiable Information (PII) and Criminal History Record Information (CHRI), what it is used for and who is allowed to access CHRI.

Other topics include purpose Codes, use of data and Attention Fields along with the requirements for each when querying CHRI information. How a Computerized Criminal History (CCH) is created.

Finally, the student will learn what Secondary Dissemination of criminal history information and why a Secondary Dissemination log must be maintained when sharing criminal history information.

1.16 CJIS Compliance



CJIS Compliance

F.S. 943 Requires FDLE CJIS Auditors to conduct Agency Audits every three years

On-Site or Correspondence

CJIS Records

Technical

Objective is to ensure compliance with CJIS Policies and Procedures and the FBI CJIS Security Policy

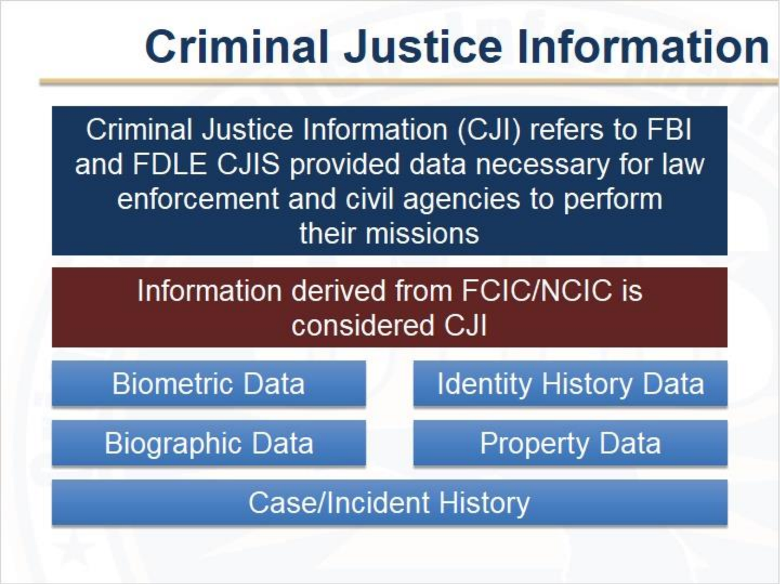
Notes:

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

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

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

1.17 Criminal Justice Information



Criminal Justice Information

Criminal Justice Information (CJI) refers to FBI and FDLE CJIS provided data necessary for law enforcement and civil agencies to perform their missions

Information derived from FCIC/NCIC is considered CJI

Biometric Data

Identity History Data

Biographic Data

Property Data

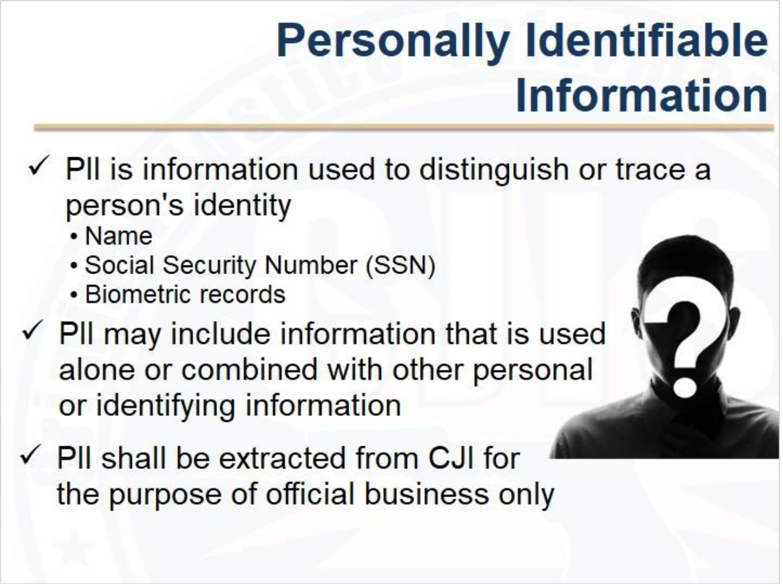
Case/Incident History

Notes:

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

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

1.18 Personally Identifiable Information



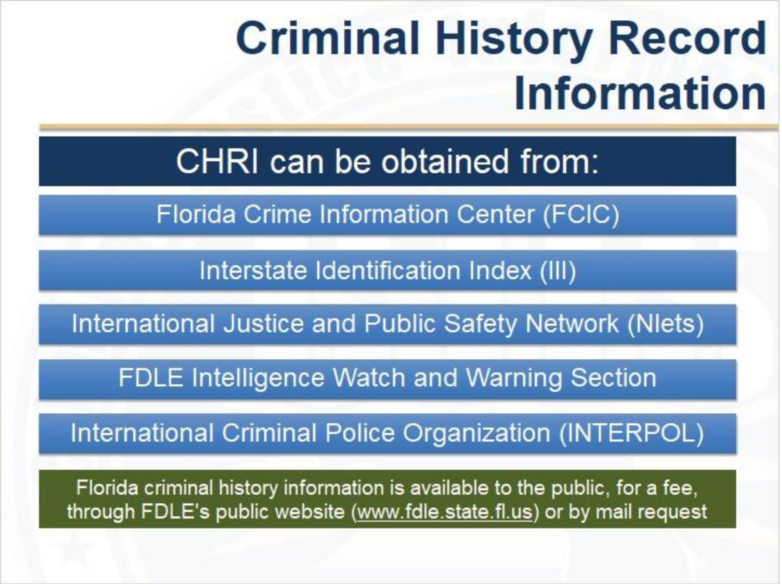
Personally Identifiable Information

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

Notes:

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

1.19 Criminal History Record Information (CHRI)



Criminal History Record Information

CHRI can be obtained from:

- Florida Crime Information Center (FCIC)
- Interstate Identification Index (III)
- International Justice and Public Safety Network (Nlets)
- FDLE Intelligence Watch and Warning Section
- International Criminal Police Organization (INTERPOL)

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

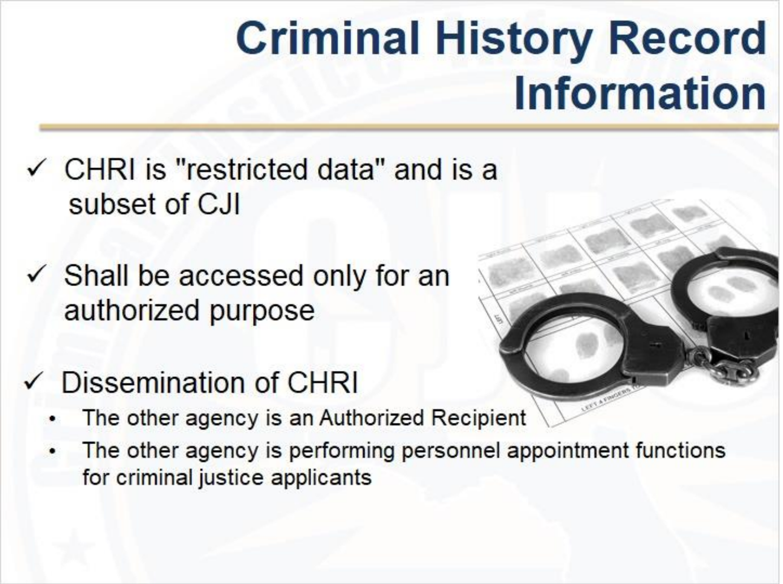
Notes:

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

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

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

1.20 Criminal History Record Information (CHRI)



Criminal History Record Information

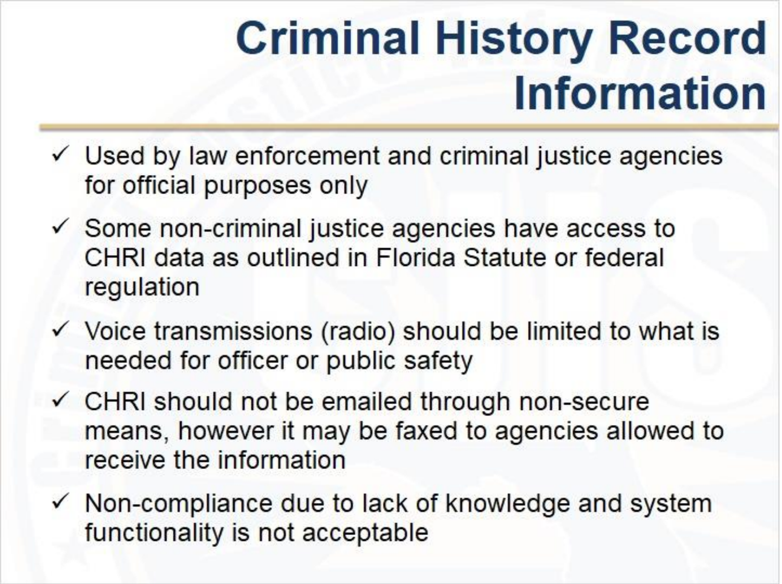
- ✓ CHRI is "restricted data" and is a subset of CJI
- ✓ Shall be accessed only for an authorized purpose
- ✓ Dissemination of CHRI
  - The other agency is an Authorized Recipient
  - The other agency is performing personnel appointment functions for criminal justice applicants

Notes:

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

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

1.21 Criminal History Record Information (CHRI)



Criminal History Record Information

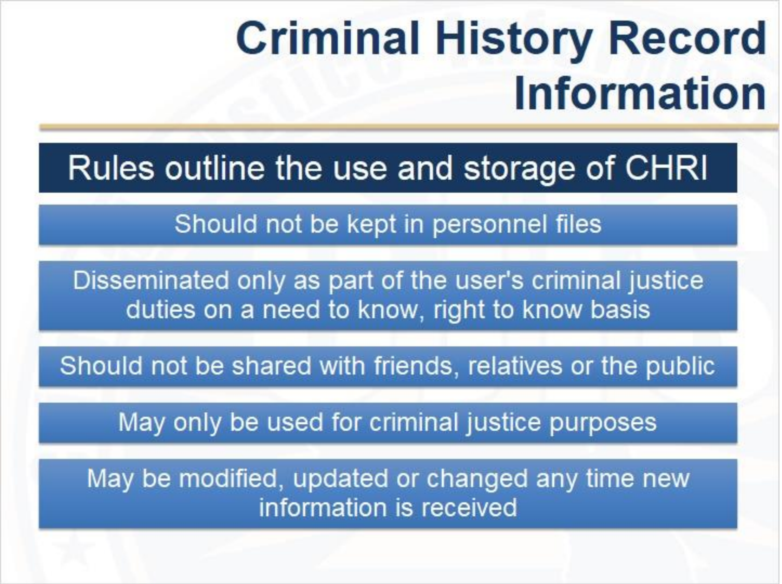
- ✓ Used by law enforcement and criminal justice agencies for official purposes only
- ✓ Some non-criminal justice agencies have access to CHRI data as outlined in Florida Statute or federal regulation
- ✓ Voice transmissions (radio) should be limited to what is needed for officer or public safety
-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

Notes:

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

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

1.22 Criminal History Record Information (CHRI)



Criminal History Record Information

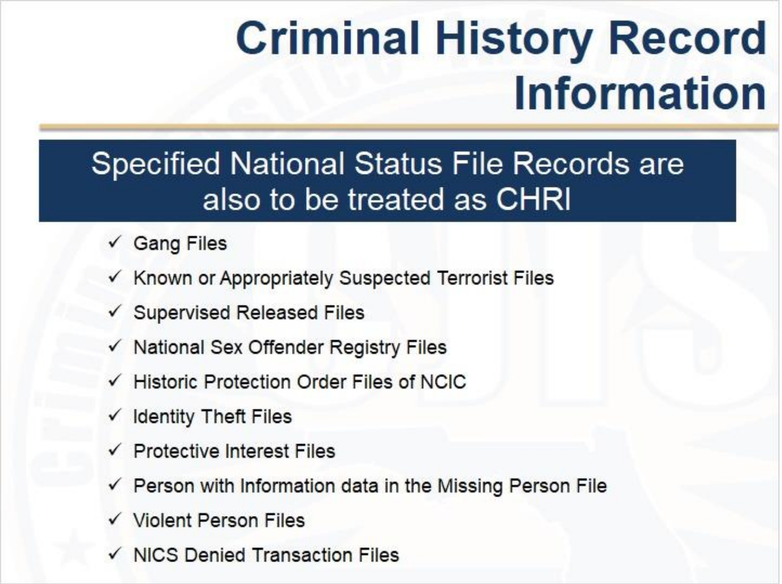
Rules outline the use and storage of CHRI

- Should not be kept in personnel files
- 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

Notes:

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

1.23 Criminal History Record Information (CHRI)



Criminal History Record Information

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

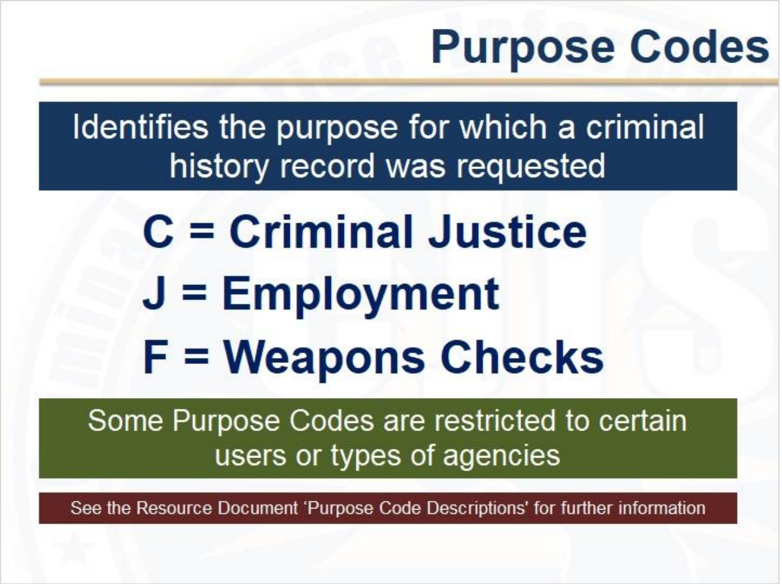
- ✓ Gang Files
- ✓ Known or Appropriately Suspected Terrorist Files
- ✓ Supervised Released Files
- ✓ National Sex Offender Registry Files
- ✓ Historic Protection Order Files of NCIC
- ✓ Identity Theft Files
- ✓ Protective Interest Files
- ✓ Person with Information data in the Missing Person File
- ✓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

Notes:

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

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

1.24 Purpose Codes



Purpose Codes

Identifies the purpose for which a criminal history record was requested

C = Criminal Justice

J = Employment

F = Weapons Checks

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

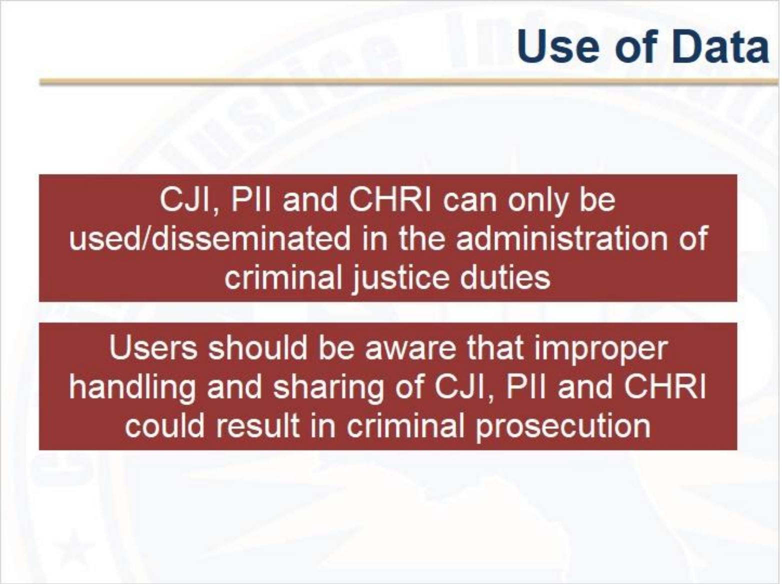
See the Resource Document 'Purpose Code Descriptions' for further information

Notes:

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

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

1.25 Use of Data



Use of Data

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

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

Notes:

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

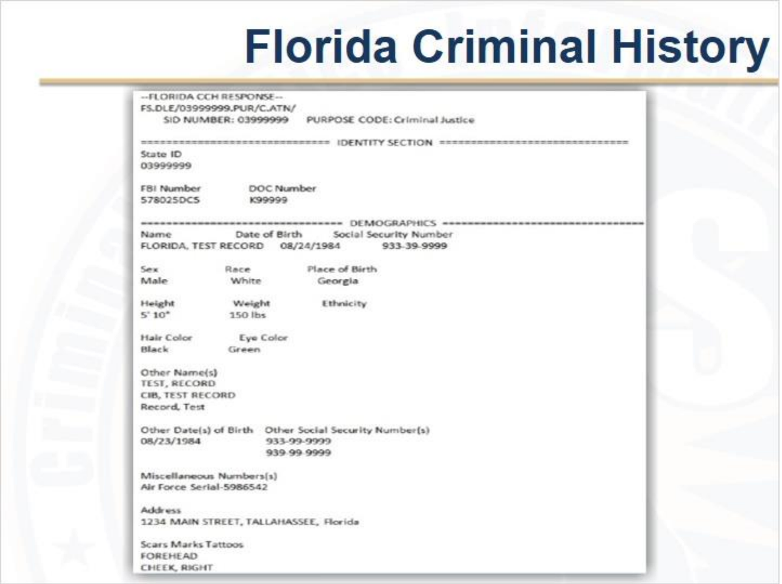
1.26 How a Florida Criminal History is Created

How a Criminal History is Created

Notes:

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

1.27 Florida Criminal History



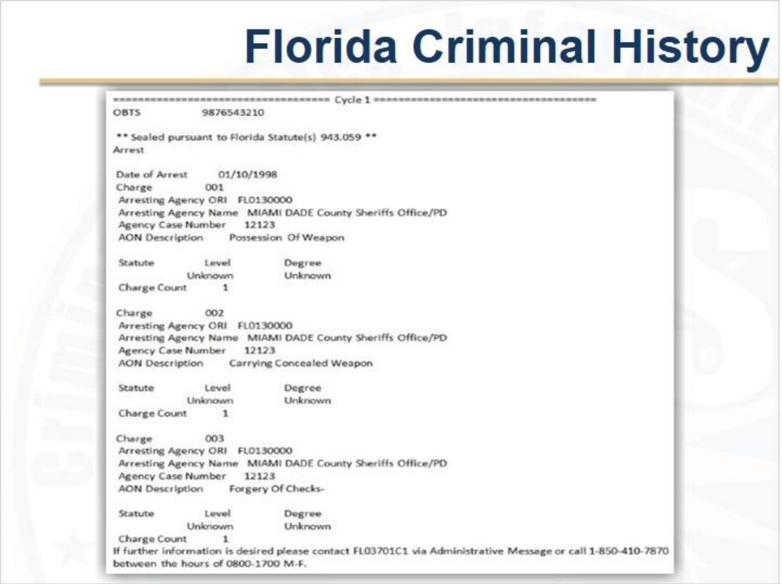
Florida Criminal History

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

============================== IDENTITY SECTION ==============================
State ID
03999999

FBI Number          DOC Number
578025DCS           K99999

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

Sex             Race            Place of Birth
Male             White            Georgia

Height           Weight           Ethnicity
5' 10"          150 lbs

Hair Color        Eye Color
Black            Green

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

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

Miscellaneous Numbers(s)
Air Force Serial-5986542

Address
1234 MAIN STREET, TALLAHASSEE, Florida

Scars Marks Tattoos
FOREHEAD
CHEEK, RIGHT
```

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.

1.28 Florida Criminal History



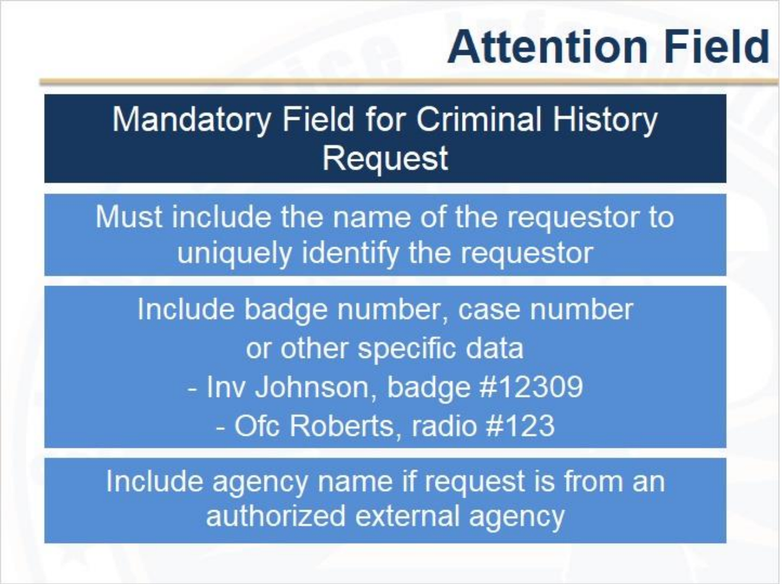
Florida Criminal History

```
=================================== Cycle 1 ===================================
OBTS              9876543210

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

 Date of Arrest        01/10/1998
 Charge               001
  Arresting Agency ORI   FL0130000
  Arresting Agency Name   MIAMI DADE County Sheriffs Office/PD
  Agency Case Number     12123
  AON Description        Possession  Of Weapon

  Statute            Level             Degree
                 Unknown            Unknown
  Charge Count          1

 Charge               002
  Arresting Agency ORI   FL0130000
  Arresting Agency Name   MIAMI DADE County Sheriffs Office/PD
  Agency Case Number     12123
  AON Description        Carrying Concealed Weapon

  Statute            Level             Degree
                 Unknown            Unknown
  Charge Count          1

 Charge               003
  Arresting Agency ORI   FL0130000
  Arresting Agency Name   MIAMI DADE County Sheriffs Office/PD
  Agency Case Number     12123
  AON Description        Forgery Of Checks-

  Statute            Level             Degree
                 Unknown            Unknown
  Charge Count          1
If further information is desired please contact FL03701C1 via Administrative Message or call 1-850-410-7870
between the hours of 0800-1700 M-F.
```

Notes:

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

1.29 Attention Field



Attention Field

Mandatory Field for Criminal History Request

Must include the name of the requestor to uniquely identify the requestor

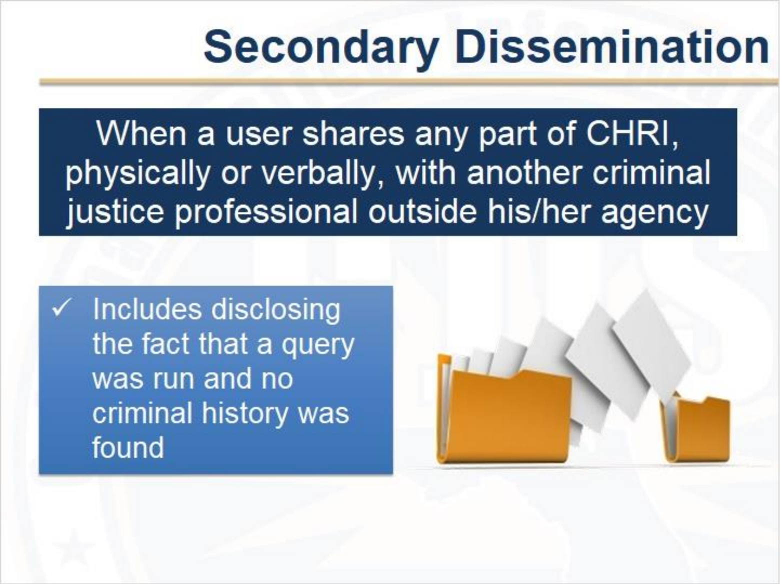
Include badge number, case number or other specific data
- Inv Johnson, badge #12309
- Ofc Roberts, radio #123

Include agency name if request is from an authorized external agency

Notes:

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

1.30 Secondary Dissemination



Secondary Dissemination

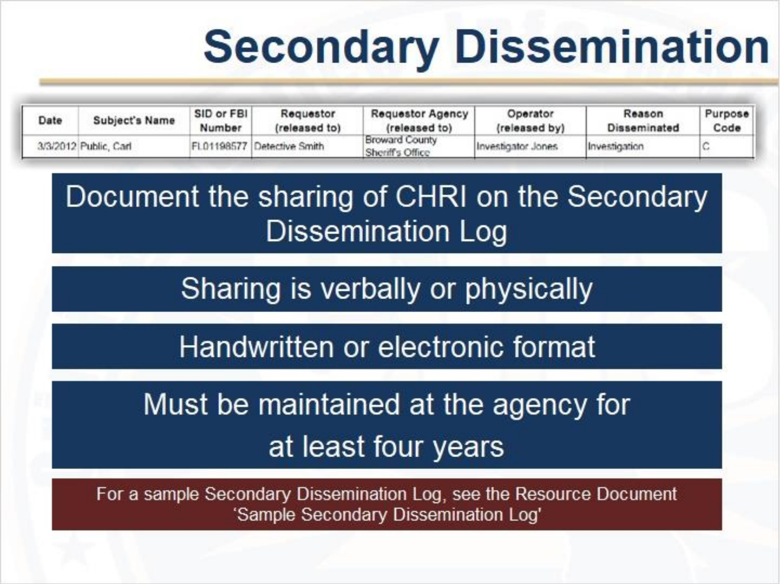
When a user shares any part of CHRI, physically or verbally, with another criminal justice professional outside his/her agency

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

Notes:

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

1.31 Secondary Dissemination Log



Secondary Dissemination

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

Document the sharing of CHRI on the Secondary Dissemination Log

Sharing is verbally or physically

Handwritten or electronic format

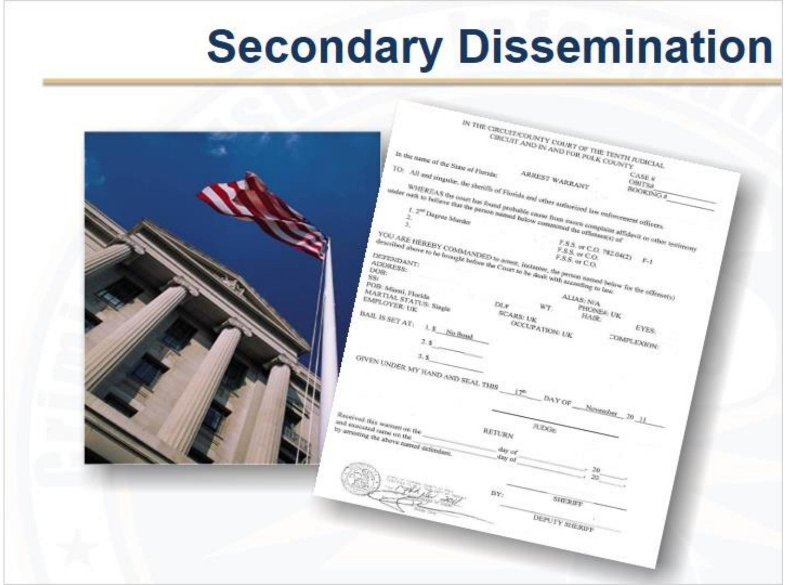
Must be maintained at the agency for at least four years

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

Notes:

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

1.32 Secondary Dissemination



Secondary Dissemination

IN THE CIRCUIT/COUNTY COURT OF THE TENTH JUDICIAL CIRCUIT AND IN AND FOR POLK COUNTY

In the name of the State of Florida: ARREST WARRANT CASE # OBTS# BOOKING #

TO: All and singular, the sheriffs of Florida and other authorized law enforcement officers.

WHEREAS the court has found probable cause from sworn complaint affidavit or other testimony under oath to believe that the person named below committed the offense(s) of

1. 2nd Degree Murder F.S.S. or C.O. 782.04(2) F-1
2. F.S.S. or C.O.
3. F.S.S. or C.O.

YOU ARE HEREBY COMMANDED to arrest, instanter, the person named below for the offense(s) described above to be brought before the Court to be dealt with according to law.

DEFENDANT:
ADDRESS:
DOB:
SS#
POB: Miami, Florida
MARTIAL STATUS: Single
EMPLOYER: UK

ALIAS: N/A
DL# WT. PHONE#: UK
SCARS: UK HAIR: EYES:
OCCUPATION: UK COMPLEXION:

BAIL IS SET AT: 1. $ No Bond
2. $
3. $

GIVEN UNDER MY HAND AND SEAL THIS 17th DAY OF November 20 11

JUDGE

RETURN

Received this warrant on the ___ day of ___ 20__
and executed same on the ___ day of ___ 20__
by arresting the above named defendant.

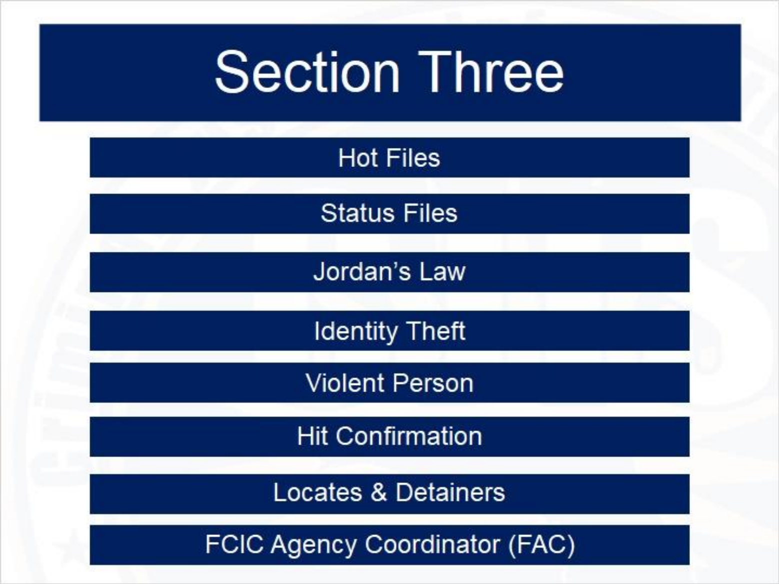
BY: SHERIFF

DEPUTY SHERIFF

Notes:

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

1.33 Section Three



Section Three

Hot Files

Status Files

Jordan’s Law

Identity Theft

Violent Person

Hit Confirmation

Locates & Detainers

FCIC Agency Coordinator (FAC)

Notes:

Section Three of the Limited Access Certification Course includes an overview of Hot File Records, Status Files, Jordan’s Law, Identity Theft, the Violent Person file, Hit Confirmations, Locates and Detainers, and the FCIC Agency Coordinator.

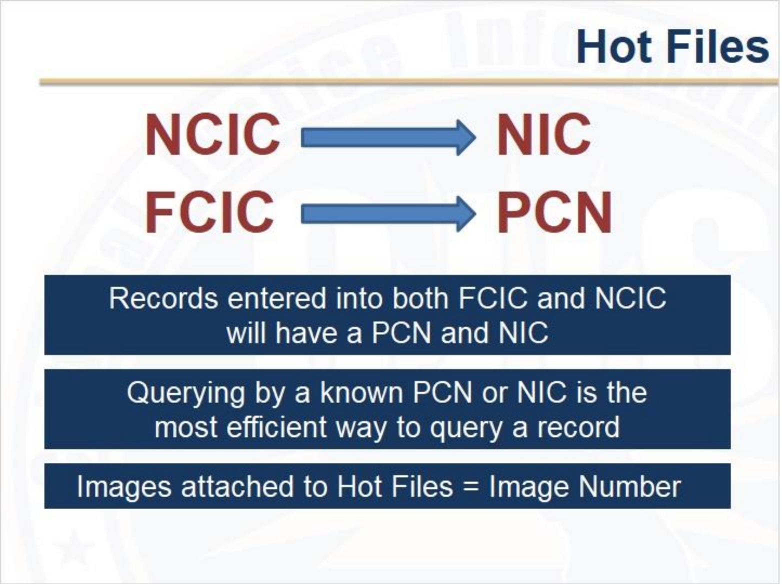
The student will learn about Hot File records and what types of information they contain.

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. The student will learn about Jordan’s Law for Missing Person entries, what the Identity Theft file is used for and the importance of the Violent Person File.

The student will also learn about Hit Confirmations, Locates and Detainers and why they are important.

Included in this section will be an overview of the roles and responsibilities of the FCIC Agency Coordinator, or FAC.

1.34 Hot Files



Hot Files

NCIC → NIC

FCIC → PCN

Records entered into both FCIC and NCIC will have a PCN and NIC

Querying by a known PCN or NIC is the most efficient way to query a record

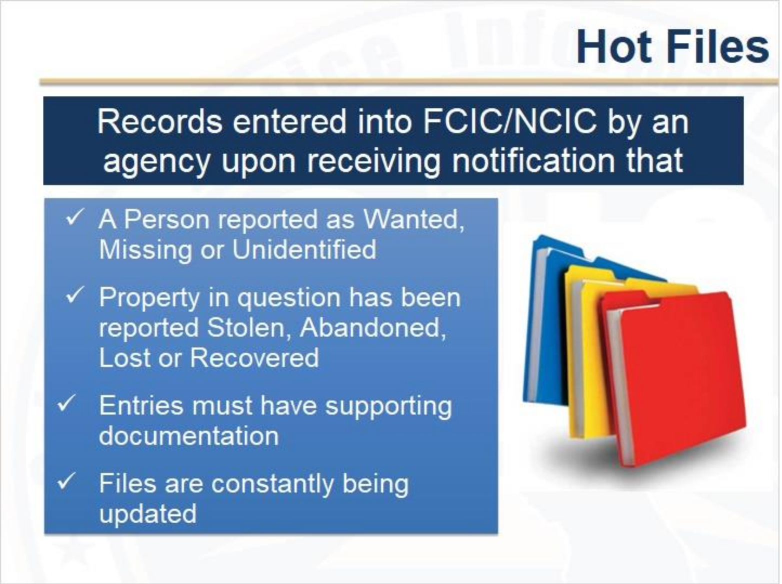
Images attached to Hot Files = Image Number

Notes:

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

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

1.35 Hot Files



Hot Files

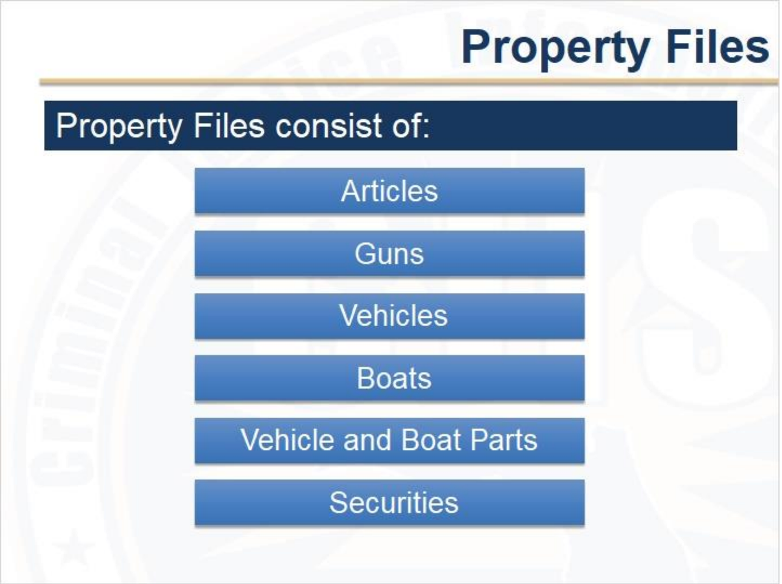
Records entered into FCIC/NCIC by an agency upon receiving notification that

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

Notes:

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

1.36 Property Files Introduction



Property Files

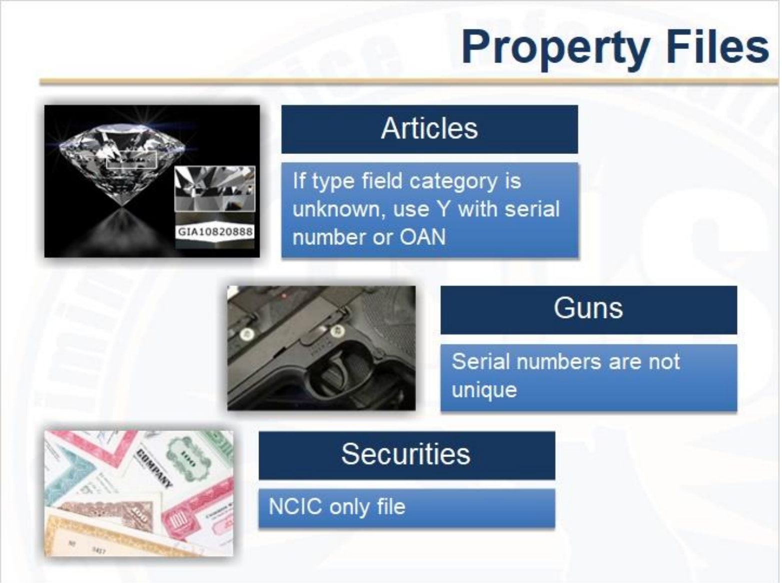
Property Files consist of:

- Articles
- Guns
- Vehicles
- Boats
- Vehicle and Boat Parts
- Securities

Notes:

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

1.37 Property Files



Property Files

Articles

If type field category is unknown, use Y with serial number or OAN

Guns

Serial numbers are not unique

Securities

NCIC only file

GIA10820888

Notes:

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

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

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

1.38 Property Files

Property Files

Vehicles

License Plates

Boats

Vehicle and Boat Parts

See the Resource Document 'Boat Registration Query' for further information

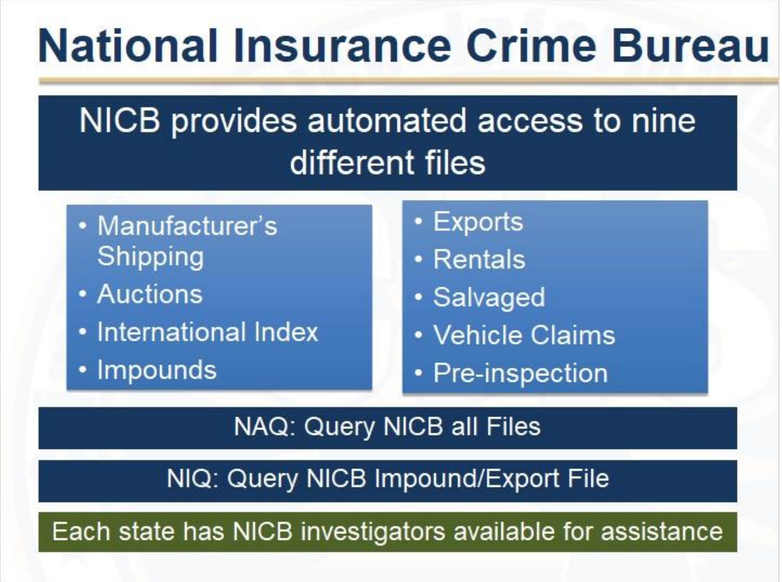
Notes:

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

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

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

1.39 NICB



National Insurance Crime Bureau

NICB provides automated access to nine different files

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

NAQ: Query NICB all Files

NIQ: Query NICB Impound/Export File

Each state has NICB investigators available for assistance

Notes:

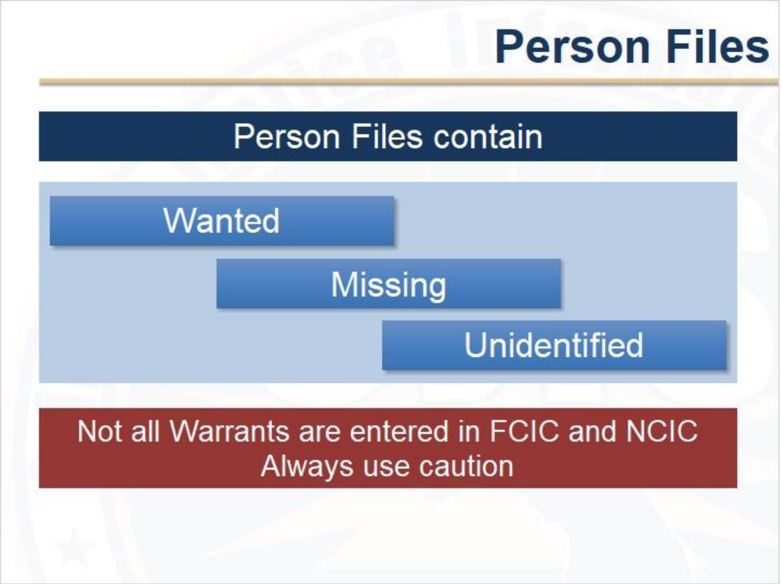
The National Insurance Crime Bureau (NICB) provides automated access to nine different files:

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

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

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

1.40 Person Files



Person Files

Person Files contain

Wanted

Missing

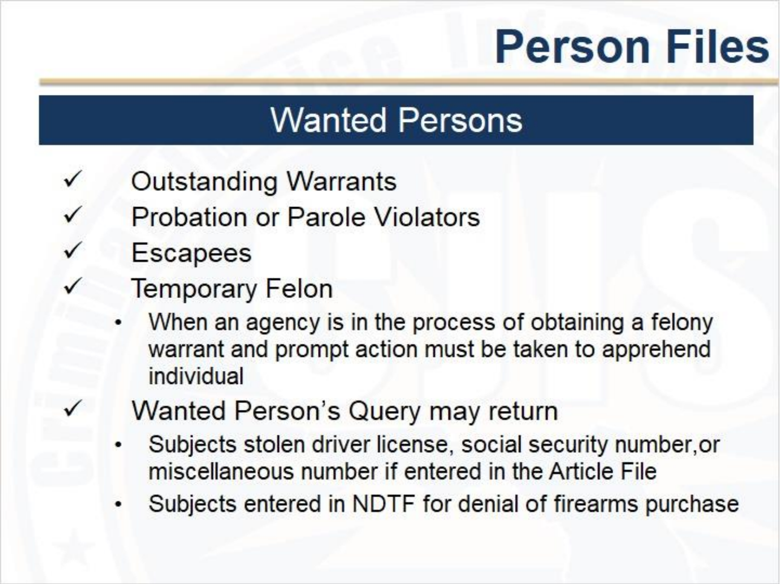
Unidentified

Not all Warrants are entered in FCIC and NCIC
Always use caution

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.

1.41 Person Files



Person Files

Wanted Persons

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

Notes:

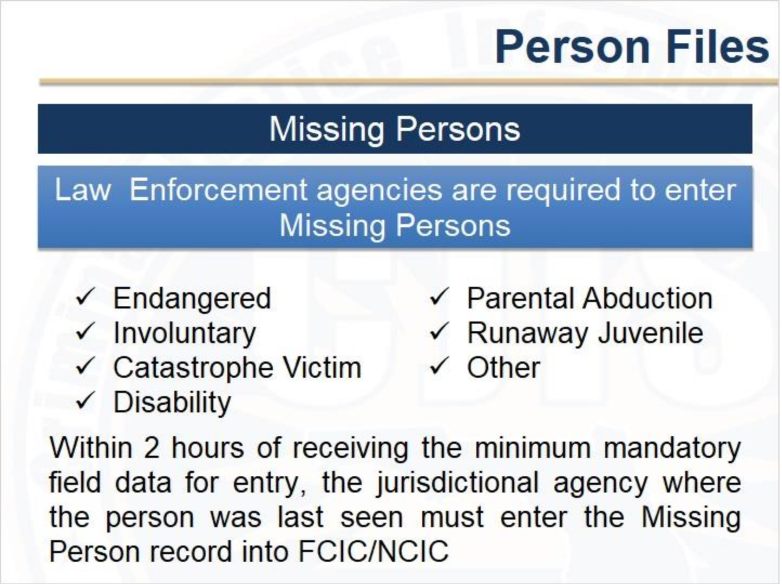
Wanted Person Files include any individual, including a juvenile who will be tried as an adult, for whom a federal, felony or serious misdemeanor warrant is outstanding, individuals that are probation and parole violators, and escapees.

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

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

Subjects that have been entered in the National Instant Criminal Background Check System (NICS) Denied Transaction File (NDTF) for denial of firearms purchase may be returned with a QW transaction. The knowledge of the denial of prohibited persons will alert the user to the subject’s tendency to possess, attempt to possess, or use of firearms. This awareness may suggest a host of possible actions or precautions that law enforcement or criminal justice agencies may want or need to take during their encounter with the subject. With the additional data, the search results may include multiple hits to the subject/detainee spanning six months.

1.42 Person Files



Person Files

Missing Persons

Law Enforcement agencies are required to enter Missing Persons

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

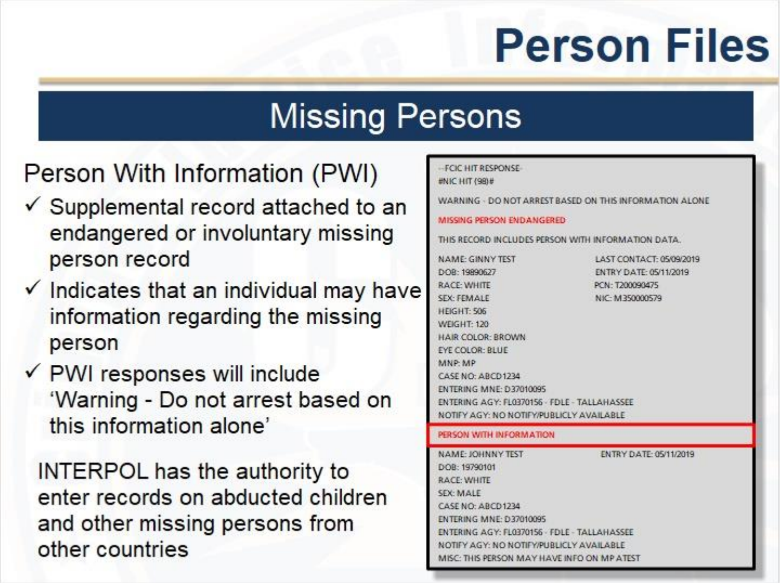
Within 2 hours of receiving the minimum mandatory field data for entry, the jurisdictional agency where the person was last seen must enter the Missing Person record into FCIC/NCIC

Notes:

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

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

1.43 Person Files



Person Files

Missing Persons

Person With Information (PWI)

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

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

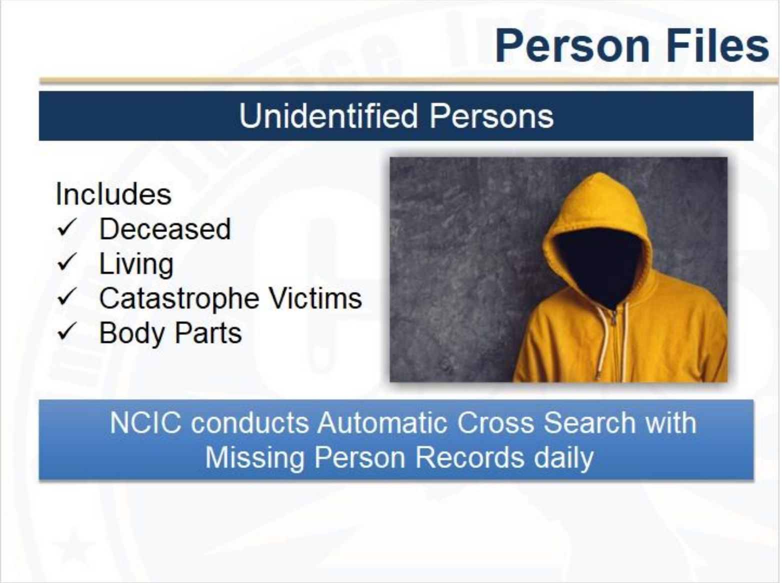
```
--FCIC HIT RESPONSE-
#NIC HIT (98)#

WARNING - DO NOT ARREST BASED ON THIS INFORMATION ALONE

MISSING PERSON ENDANGERED

THIS RECORD INCLUDES PERSON WITH INFORMATION DATA.

NAME: GINNY TEST                        LAST CONTACT: 05/09/2019
DOB: 19890627                           ENTRY DATE: 05/11/2019
RACE: WHITE                             PCN: T200090475
SEX: FEMALE                             NIC: M350000579
HEIGHT: 506
WEIGHT: 120
HAIR COLOR: BROWN
EYE COLOR: BLUE
MNP: MP
CASE NO: ABCD1234
ENTERING MNE: D37010095
ENTERING AGY: FL0370156 - FDLE - TALLAHASSEE
NOTIFY AGY: NO NOTIFY/PUBLICLY AVAILABLE

PERSON WITH INFORMATION

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

Notes:

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

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

1.44 Person Files



Person Files

Unidentified Persons

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

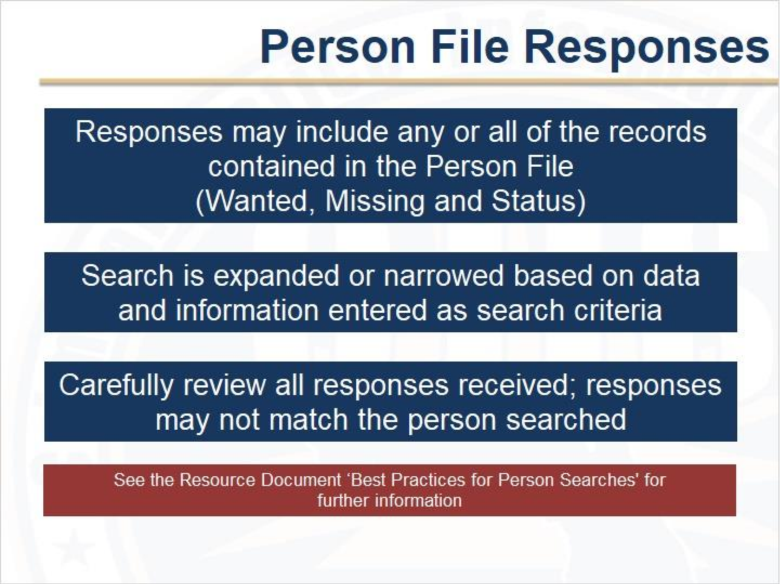
NCIC conducts Automatic Cross Search with Missing Person Records daily

Notes:

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

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

1.45 Person Files



Person File Responses

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

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

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

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

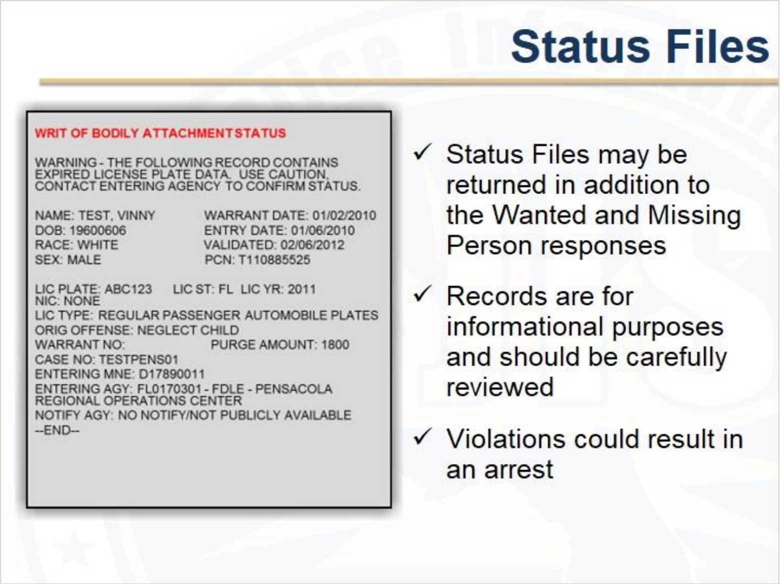
Notes:

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

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

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

1.46 Status Files



Status Files

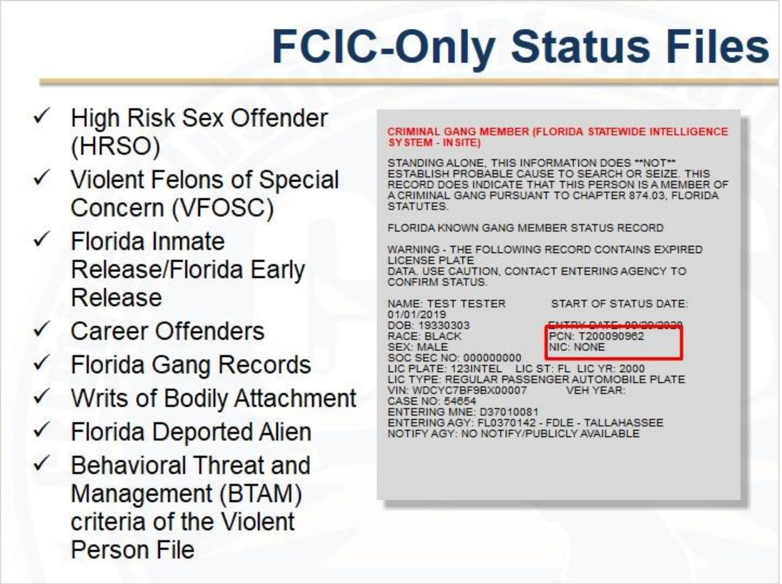
```
WRIT OF BODILY ATTACHMENTSTATUS

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

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

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

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

Notes:

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

1.47 FCIC-Only Status Files



FCIC-Only Status Files

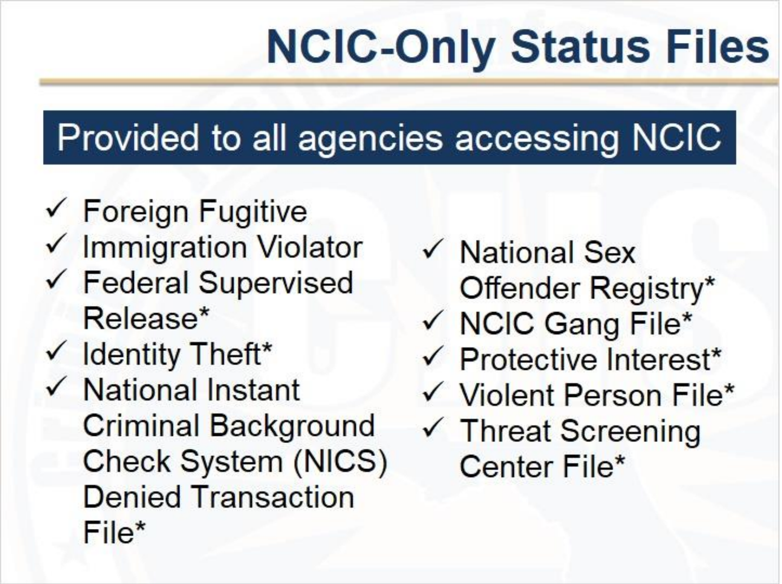
- ✓ High Risk Sex Offender (HRSO)
- ✓ Violent Felons of Special Concern (VFOSC)
- ✓ Florida Inmate Release/Florida Early Release
- ✓ Career Offenders
- ✓ Florida Gang Records
- ✓ Writs of Bodily Attachment
- ✓ Florida Deported Alien
- ✓ Behavioral Threat and Management (BTAM) criteria of the Violent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

```
CRIMINAL GANG MEMBER (FLORIDA STATEWIDE INTELLIGENCE
SYSTEM - 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:
01/01/2019
DOB: 19330303              ENTRY DATE: 09/30/2020
RACE: BLACK                PCN: T200090962
SEX: MALE                  NIC: NONE
SOC SEC NO: 000000000
LIC PLATE: 123INTEL    LIC ST: FL  LIC YR: 2000
LIC TYPE: REGULAR PASSENGER AUTOMOBILE PLATE
VIN: WDCYC7BF9BX00007          VEH YEAR:
CASE NO: 54654
ENTERING MNE: D37010081
ENTERING AGY: FL0370142 - FDLE - TALLAHASSEE
NOTIFY AGY: NO NOTIFY/PUBLICLY AVAILABLE
```

Notes:

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

1.48 NCIC-Only Status Files



NCIC-Only Status Files

Provided to all agencies accessing NCIC

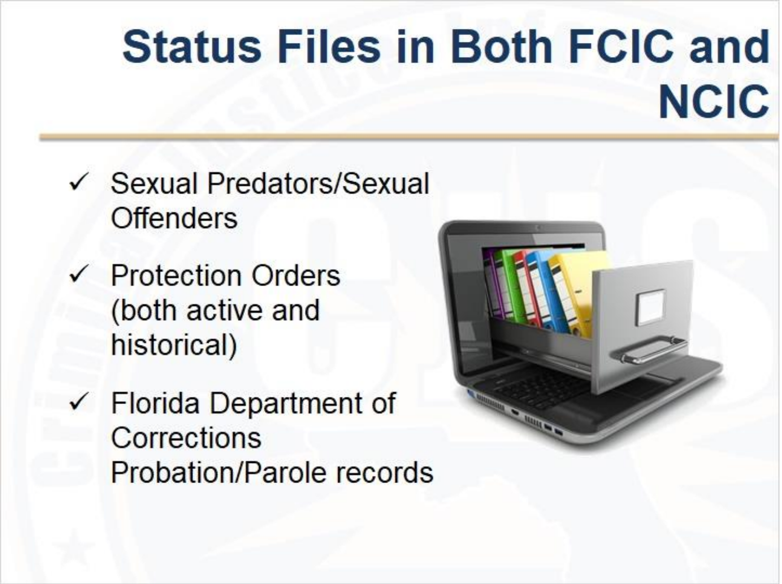
- ✓ Foreign Fugitive
- ✓ Immigration Violator
- ✓ Federal Supervised Release*
- ✓ Identity Theft*
- ✓ National Instant Criminal Background Check System (NICS) Denied Transaction File*
- ✓ National Sex Offender Registry*
- ✓ NCIC Gang File*
- ✓ Protective Interest*
- ✓ Violent Person File*
- ✓ Threat Screening Center File*

Notes:

NCIC-Only Status Files are provided to all agencies accessing NCIC. These files include Foreign Fugitive, Immigration Violator, Federal Supervised Release, Identity Theft, National Instant Criminal Background Check System (NICS) Denied Transaction File, National Sex Offender Registry, NCIC Gang file, Protective Interest, Violent Person File, and the Threat Screening Center file. It is extremely important to note that any Threat Screening Center 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 safety or public safety is an issue.

1.49 Status Files in both FCIC and NCIC



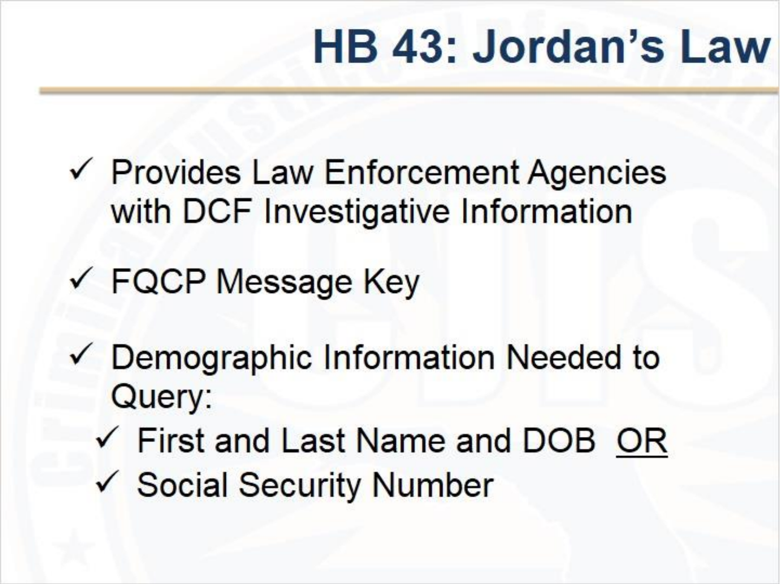
Status Files in Both FCIC and NCIC

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

Notes:

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

1.50 Jordan's Law



HB 43: Jordan's Law

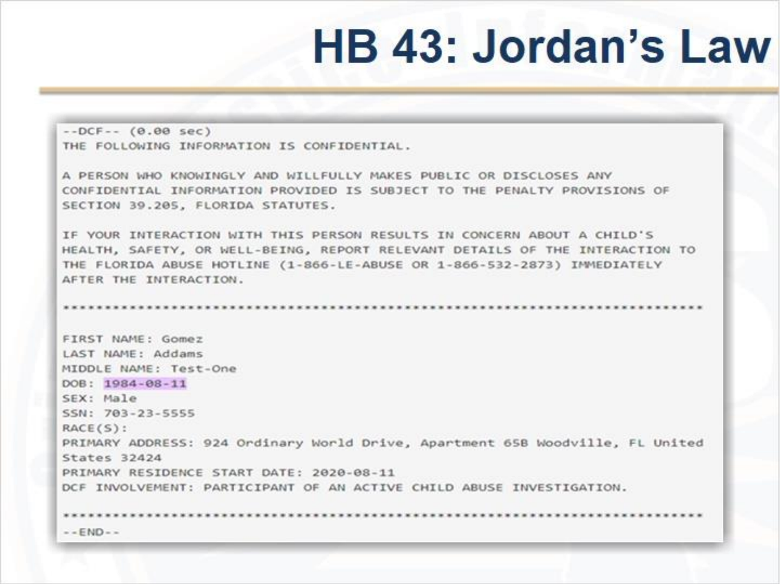
- ✓ Provides Law Enforcement Agencies with DCF Investigative Information
- ✓ FQCP Message Key
- ✓ Demographic Information Needed to Query:
  - ✓ First and Last Name and DOB <u>OR</u>
  - ✓ Social Security Number

Notes:

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

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

1.51 Jordan's Law



HB 43: Jordan's Law

```
--DCF-- (0.00 sec)
THE FOLLOWING INFORMATION IS CONFIDENTIAL.

A PERSON WHO KNOWINGLY AND WILLFULLY MAKES PUBLIC OR DISCLOSES ANY
CONFIDENTIAL INFORMATION PROVIDED IS SUBJECT TO THE PENALTY PROVISIONS OF
SECTION 39.205, FLORIDA STATUTES.

IF YOUR INTERACTION WITH THIS PERSON RESULTS IN CONCERN ABOUT A CHILD'S
HEALTH, SAFETY, OR WELL-BEING, REPORT RELEVANT DETAILS OF THE INTERACTION TO
THE FLORIDA ABUSE HOTLINE (1-866-LE-ABUSE OR 1-866-532-2873) IMMEDIATELY
AFTER THE INTERACTION.

****************************************************************************

FIRST NAME: Gomez
LAST NAME: Addams
MIDDLE NAME: Test-One
DOB: 1984-08-11
SEX: Male
SSN: 703-23-5555
RACE(S):
PRIMARY ADDRESS: 924 Ordinary World Drive, Apartment 658 Woodville, FL United
States 32424
PRIMARY RESIDENCE START DATE: 2020-08-11
DCF INVOLVEMENT: PARTICIPANT OF AN ACTIVE CHILD ABUSE INVESTIGATION.

****************************************************************************
--END--
```

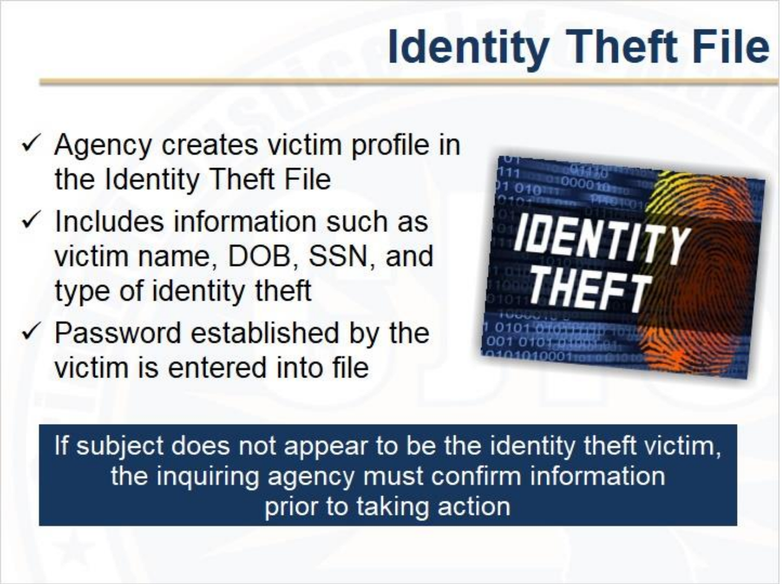
Notes:

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

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

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

1.52 Identity Theft



IDENTITY
THEFT

Identity Theft File

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

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

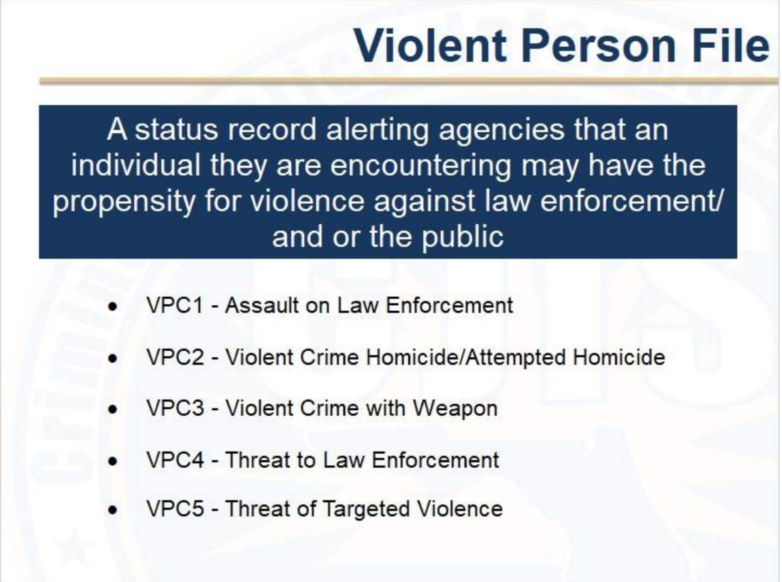
Notes:

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

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

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

1.53 Violent Person File



Violent Person File

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

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

Notes:

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

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

VPC 1: Assault on Law Enforcement: Offender has been convicted for assault or murder/homicide of a law enforcement officer, fleeing, resisting arrest, or any such statute which involves violence against law enforcement.

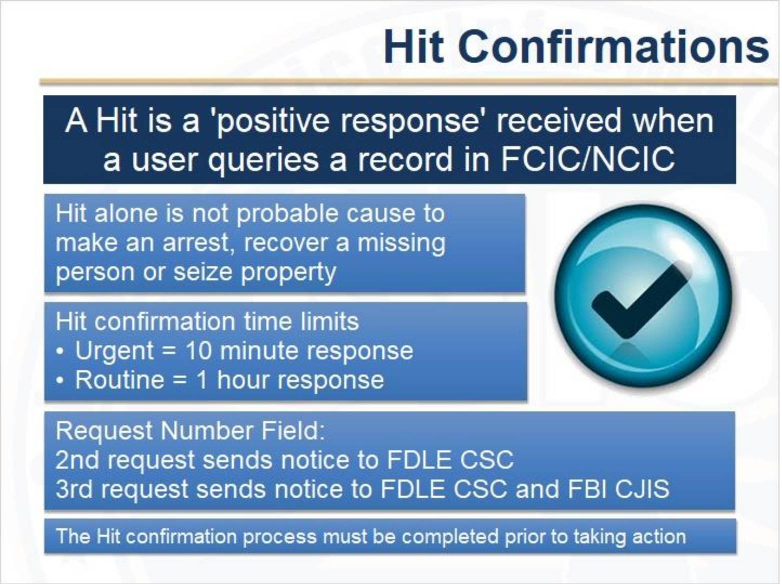
VPC 2: Violent Crime Homicide/Attempted Homicide: Offender has been convicted of a violent offense against a person to include homicide and attempted homicide.

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

VPC 4: Threat to Law Enforcement: A law enforcement agency, based on its official investigative duties, reasonably believes that the individual has seriously expressed his or her intent to commit an act of unlawful violence against a member of the law enforcement community.

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

1.54 Hit Confirmations



Hit Confirmations

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

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

Hit confirmation time limits
- Urgent = 10 minute response
- Routine = 1 hour response

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

The Hit confirmation process must be completed prior to taking action

Notes:

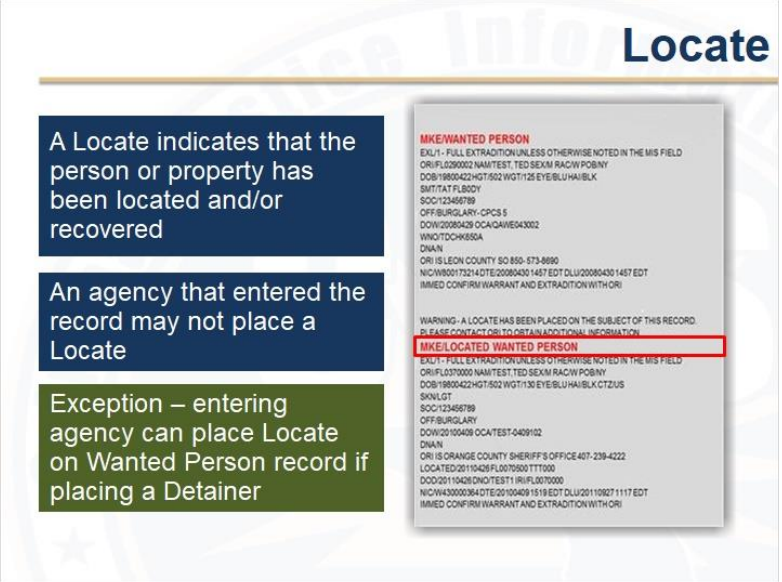
A hit is a “positive response” received when a user queries person or property records from FCIC and NCIC. A hit alone is not probable cause to make an arrest, however, a confirmed or verified hit may be adequate grounds to arrest a person, recover a missing person, or recover stolen property depending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

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

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

Before an agency can take any official action on a Hot File record hit, the Hit Confirmation process must be completed, including receiving a Hit Confirmation Response from the entering agency. The recovering agency should not place a locate or recover a person or property unless a Hit Confirmation Response has been received.

1.55 Locate



Locate

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

An agency that entered the record may not place a Locate

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

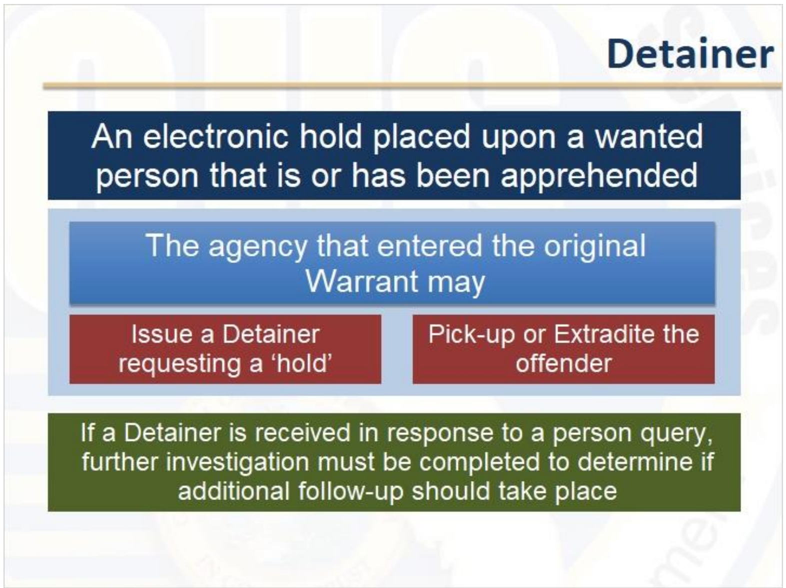
```
MKE/WANTED PERSON
EXL/1 - FULL EXTRADITION UNLESS OTHERWISE NOTED IN THE MIS FIELD
ORI/FL0290002 NAM/TEST, TED SEX/M RAC/W POB/NY
DOB/19800422 HGT/502 WGT/125 EYE/BLU HAI/BLK
SMT/TAT FLBODY
SOC/123456789
OFF/BURGLARY-CPCS 5
DOW/20080429 OCA/QAWE043002
WNO/TDCHK650A
DNA/N
ORI IS LEON COUNTY SO 850-573-8690
NIC/W800173214 DTE/20080430 1457 EDT DLU/20080430 1457 EDT
IMMED CONFIRM WARRANT AND EXTRADITION WITH ORI


WARNING - A LOCATE HAS BEEN PLACED ON THE SUBJECT OF THIS RECORD.
PLEASE CONTACT ORI TO OBTAIN ADDITIONAL INFORMATION
MKE/LOCATED WANTED PERSON
EXL/1 - FULL EXTRADITION UNLESS OTHERWISE NOTED IN THE MIS FIELD
ORI/FL0370000 NAM/TEST, TED SEX/M RAC/W POB/NY
DOB/19800422 HGT/502 WGT/130 EYE/BLU HAI/BLK CTZ/US
SKN/LGT
SOC/123456789
OFF/BURGLARY
DOW/20100409 OCA/TEST-0409102
DNA/N
ORI IS ORANGE COUNTY SHERIFF'S OFFICE 407-239-4222
LOCATED/20110426 FL0070500 TTT000
DOD/20110426 DNO/TEST1 IRI/FL0070000
NIC/W430000364 DTE/20100409 1519 EDT DLU/20110927 1117 EDT
IMMED CONFIRM WARRANT AND EXTRADITION WITH ORI
```

Notes:

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

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

1.56 Detainer



Detainer

An electronic hold placed upon a wanted person that is or has been apprehended

The agency that entered the original Warrant may

Issue a Detainer requesting a 'hold'

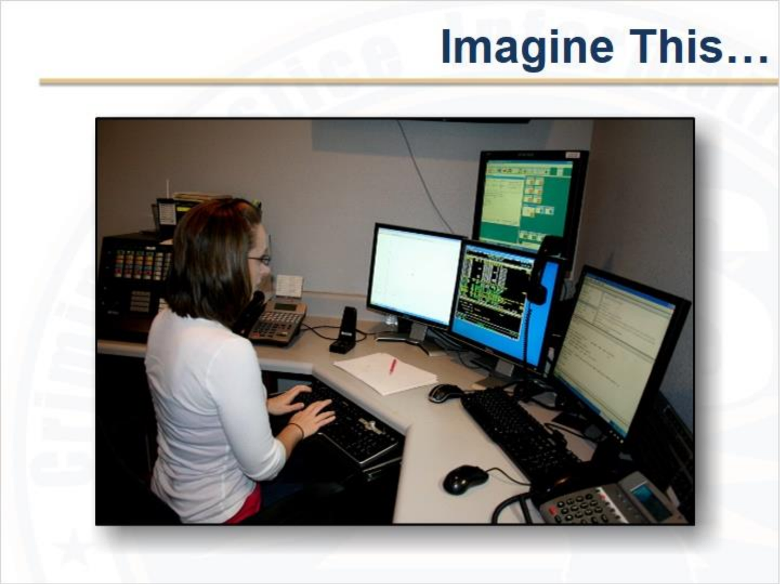
Pick-up or Extradite the offender

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

Notes:

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

1.57 Imagine this…

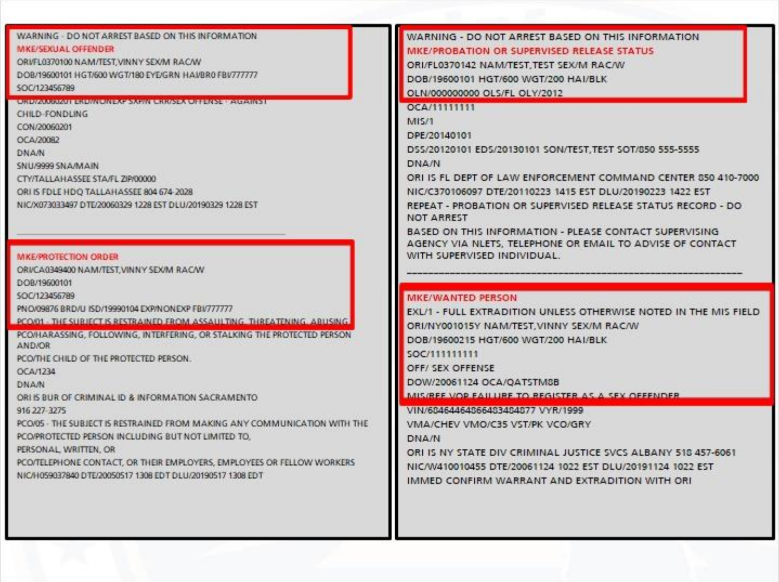


Imagine This…

Notes:

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

1.58 Imagine this scenario continued...



```
WARNING - DO NOT ARREST BASED ON THIS INFORMATION
MKE/SEXUAL OFFENDER
ORI/FL0370100 NAM/TEST,VINNY SEX/M RAC/W
DOB/19600101 HGT/600 WGT/180 EYE/GRN HAI/BR0 FBI/777777
SOC/123456789
ORD/20060201 ERD/NONEXP SXP/N CRR/SEX OFFENSE - AGAINST
CHILD-FONDLING
CON/20060201
OCA/20082
DNA/N
SNU/9999 SNA/MAIN
CTY/TALLAHASSEE STA/FL ZIP/00000
ORI IS FDLE HDQ TALLAHASSEE 804 674-2028
NIC/X073033497 DTE/20060329 1228 EST DLU/20190329 1228 EST

MKE/PROTECTION ORDER
ORI/CA0349400 NAM/TEST,VINNY SEX/M RAC/W
DOB/19600101
SOC/123456789
PNO/09876 BRD/U ISD/19990104 EXP/NONEXP FBI/777777
PCO/01 - THE SUBJECT IS RESTRAINED FROM ASSAULTING, THREATENING, ABUSING
PCO/HARASSING, FOLLOWING, INTERFERING, OR STALKING THE PROTECTED PERSON
AND/OR
PCO/THE CHILD OF THE PROTECTED PERSON.
OCA/1234
DNA/N
ORI IS BUR OF CRIMINAL ID & INFORMATION SACRAMENTO
916 227-3275
PCO/05 - THE SUBJECT IS RESTRAINED FROM MAKING ANY COMMUNICATION WITH THE
PCO/PROTECTED PERSON INCLUDING BUT NOT LIMITED TO,
PERSONAL, WRITTEN, OR
PCO/TELEPHONE CONTACT, OR THEIR EMPLOYERS, EMPLOYEES OR FELLOW WORKERS
NIC/H059037840 DTE/20050517 1308 EDT DLU/20190517 1308 EDT
```

```
WARNING - DO NOT ARREST BASED ON THIS INFORMATION
MKE/PROBATION OR SUPERVISED RELEASE STATUS
ORI/FL0370142 NAM/TEST,TEST SEX/M RAC/W
DOB/19600101 HGT/600 WGT/200 HAI/BLK
OLN/000000000 OLS/FL OLY/2012
OCA/11111111
MIS/1
DPE/20140101
DSS/20120101 EDS/20130101 SON/TEST,TEST SOT/850 555-5555
DNA/N
ORI IS FL DEPT OF LAW ENFORCEMENT COMMAND CENTER 850 410-7000
NIC/C370106097 DTE/20110223 1415 EST DLU/20190223 1422 EST
REPEAT - PROBATION OR SUPERVISED RELEASE STATUS RECORD - DO
NOT ARREST
BASED ON THIS INFORMATION - PLEASE CONTACT SUPERVISING
AGENCY VIA NLETS, TELEPHONE OR EMAIL TO ADVISE OF CONTACT
WITH SUPERVISED INDIVIDUAL.
-----------------------------------------------------------------
MKE/WANTED PERSON
EXL/1 - FULL EXTRADITION UNLESS OTHERWISE NOTED IN THE MIS FIELD
ORI/NY001015Y NAM/TEST,VINNY SEX/M RAC/W
DOB/19600215 HGT/600 WGT/200 HAI/BLK
SOC/111111111
OFF/ SEX OFFENSE
DOW/20061124 OCA/QATSTM8B
MIS/REF VOP FAILURE TO REGISTER AS A SEX OFFENDER
VIN/60464464866483404877 VYR/1999
VMA/CHEV VMO/C35 VST/PK VCO/GRY
DNA/N
ORI IS NY STATE DIV CRIMINAL JUSTICE SVCS ALBANY 518 457-6061
NIC/W410010455 DTE/20061124 1022 EST DLU/20191124 1022 EST
IMMED CONFIRM WARRANT AND EXTRADITION WITH ORI
```

Notes:

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

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

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

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

1.59 FCIC Agency Coordinator

FCIC Agency Coordinator

Agency's CJIS point of contact

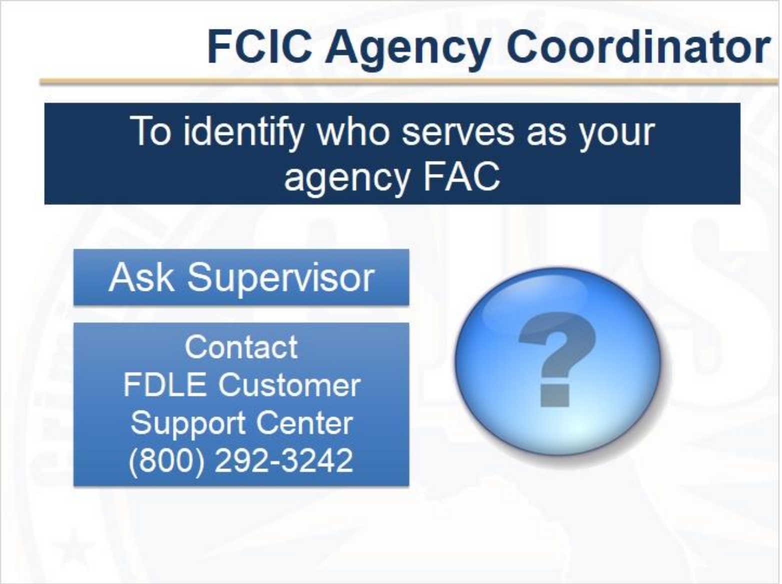
Liaison with FDLE as it relates to FCIC/NCIC

Ensures agency user compliance for FCIC/ NCIC, and Nlets systems

Notes:

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

1.60 FCIC Agency Coordinator



FCIC Agency Coordinator

To identify who serves as your agency FAC

Ask Supervisor

Contact FDLE Customer Support Center (800) 292-3242

Notes:

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

1.61 Section Four

Section Four

Delayed Inquires

System Identifiers

Administrative Communication

Alerts

Concealed Weapons

Investigative Tool

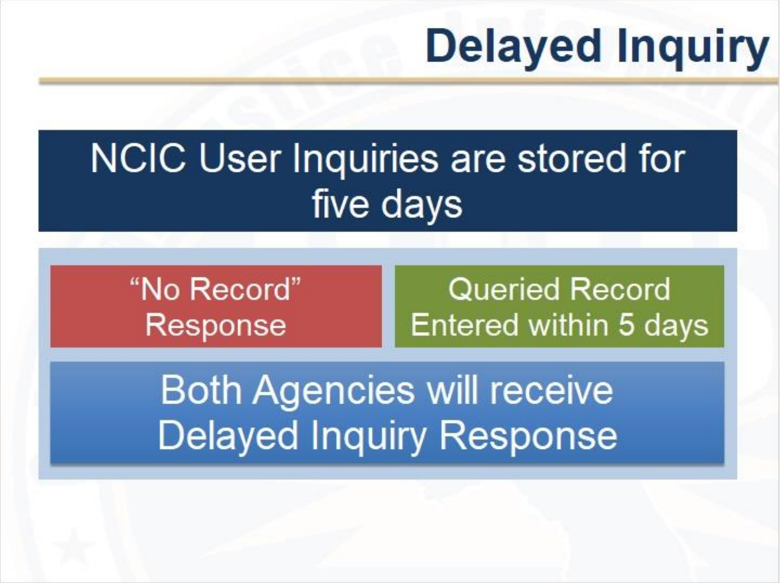
Notes:

Section Four of the Limited Access Certification Course includes an overview of Delayed Inquiries, System Identifiers, different types of Administrative Communication 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.

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 days

"No Record" Response

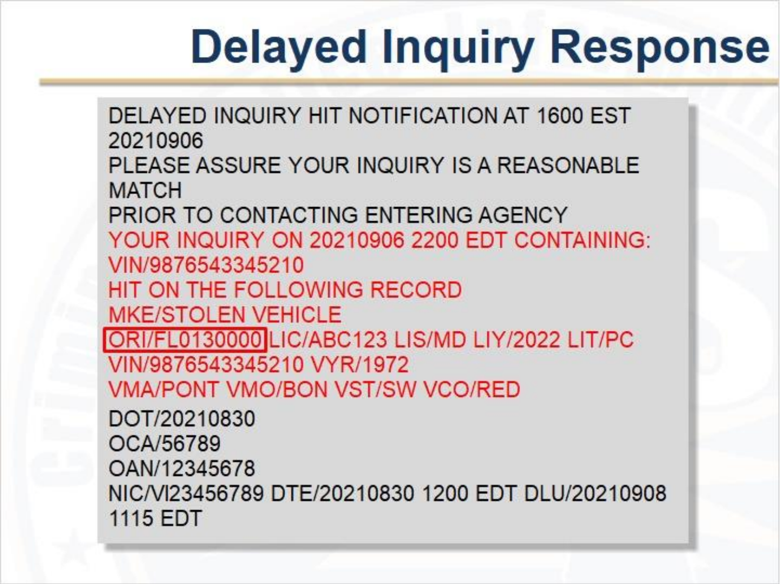
Queried Record Entered within 5 days

Both Agencies will receive Delayed Inquiry Response

Notes:

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

1.63 Delayed Inquiry Response



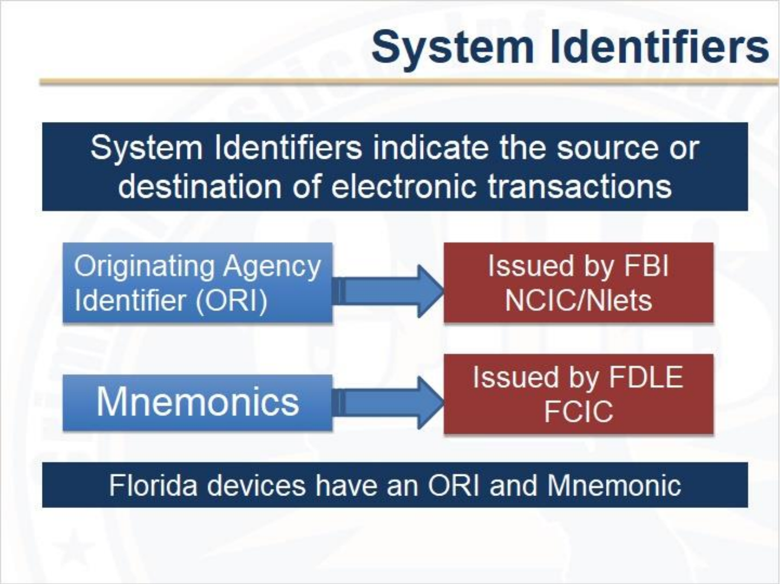
Delayed Inquiry Response

```
DELAYED INQUIRY HIT NOTIFICATION AT 1600 EST
20210906
PLEASE ASSURE YOUR INQUIRY IS A REASONABLE
MATCH
PRIOR TO CONTACTING ENTERING AGENCY
YOUR INQUIRY ON 20210906 2200 EDT CONTAINING:
VIN/9876543345210
HIT ON THE FOLLOWING RECORD
MKE/STOLEN VEHICLE
ORI/FL0130000 LIC/ABC123 LIS/MD LIY/2022 LIT/PC
VIN/9876543345210 VYR/1972
VMA/PONT VMO/BON VST/SW VCO/RED
DOT/20210830
OCA/56789
OAN/12345678
NIC/VI23456789 DTE/20210830 1200 EDT DLU/20210908
1115 EDT
```

Notes:

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

1.64 System Identifiers



System Identifiers

System Identifiers indicate the source or destination of electronic transactions

Originating Agency Identifier (ORI) → Issued by FBI NCIC/Nlets

Mnemonics → Issued by FDLE FCIC

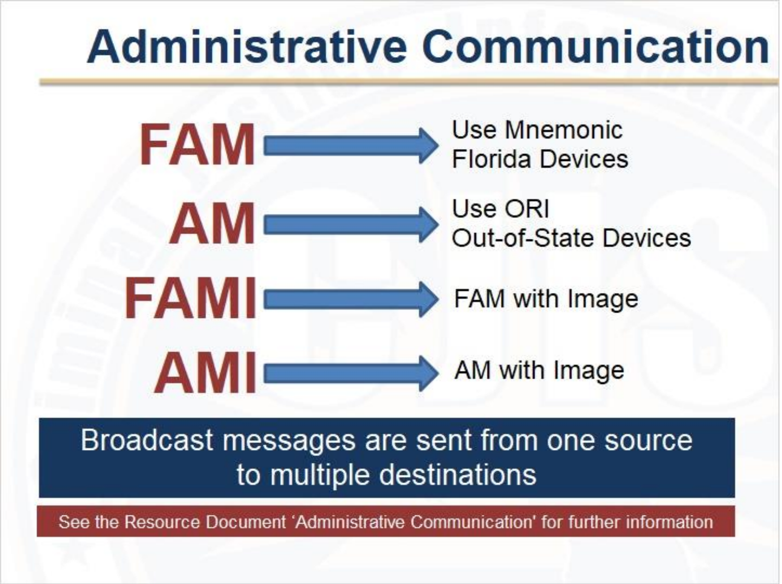
Florida devices have an ORI and Mnemonic

Notes:

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

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

1.65 Administrative Communication



Administrative Communication

FAM → Use Mnemonic Florida Devices

AM → Use ORI Out-of-State Devices

FAMI → FAM with Image

AMI → AM with Image

Broadcast messages are sent from one source to multiple destinations

See the Resource Document 'Administrative Communication' for further information

Notes:

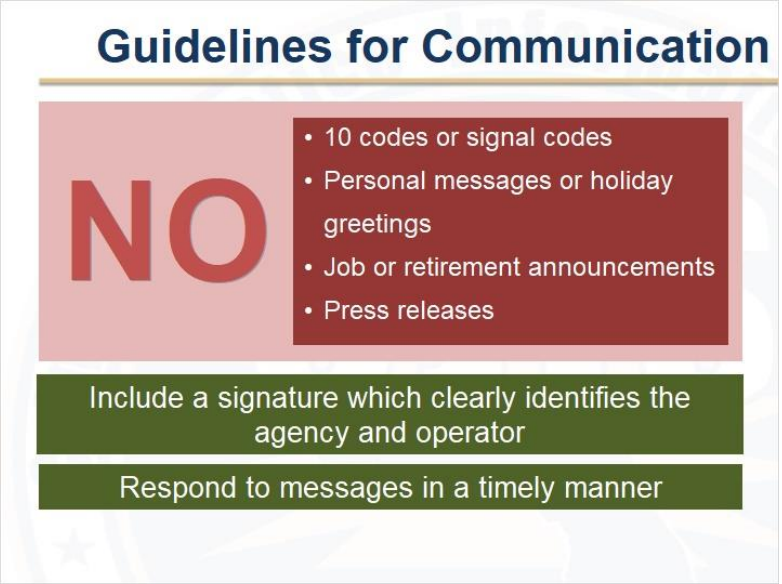
Administrative communications are FCIC and NCIC free text messages. There are two message keys used for administrative communication: A Florida Administrative Message, or FAM, uses mnemonics to identify the source and destination of a message, and should be used when the sender and recipient are both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

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

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

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

1.66 Guidelines for Communication



Guidelines for Communication

NO

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

Include a signature which clearly identifies the agency and operator

Respond to messages in a timely manner

Notes:

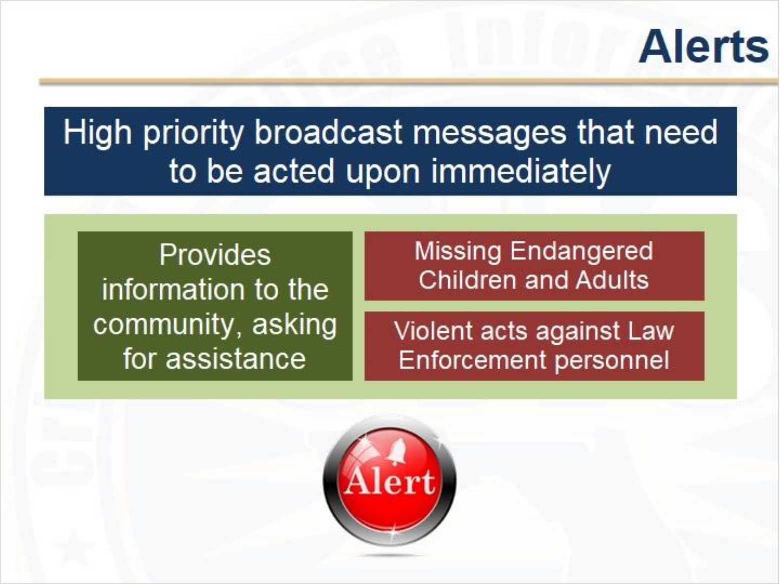
Users must follow basic guidelines when sending an administrative communication. These guidelines include using plain English, not using 10 codes or signal codes, not sending non-law enforcement related information such as personal messages, holiday greetings, job or retirement notices, and press releases.

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

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

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

1.67 Alerts Introduction



Alerts

High priority broadcast messages that need to be acted upon immediately

Provides information to the community, asking for assistance

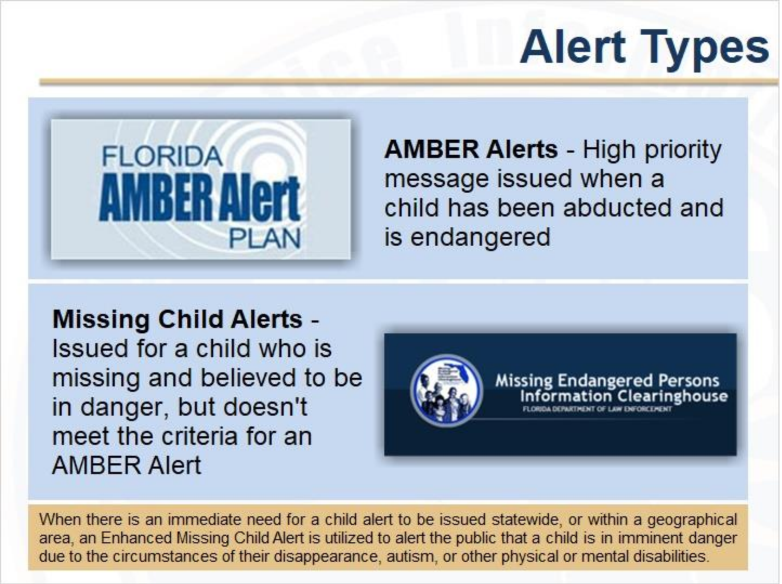
Missing Endangered Children and Adults

Violent acts against Law Enforcement personnel

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 Alert Types


FLORIDA
AMBER Alert
PLAN
Missing Endangered Persons
Information Clearinghouse
FLORIDA DEPARTMENT OF LAW ENFORCEMENT

Alert Types

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

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

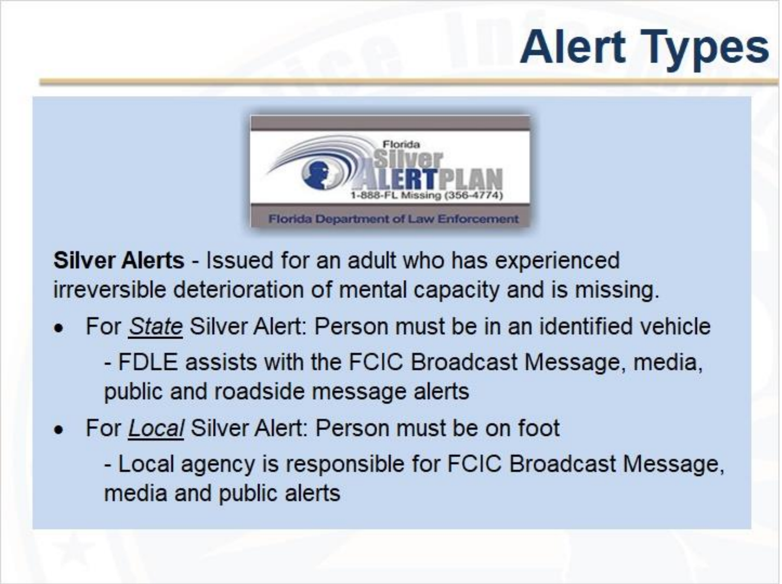
When there is an immediate need for a child alert to be issued statewide, or within a geographical area, an Enhanced Missing Child Alert is utilized to alert the public that a child is in imminent danger due to the circumstances of their disappearance, autism, or other physical or mental disabilities.

Notes:

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

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

1.69 Alert Types


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

Alert Types

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

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

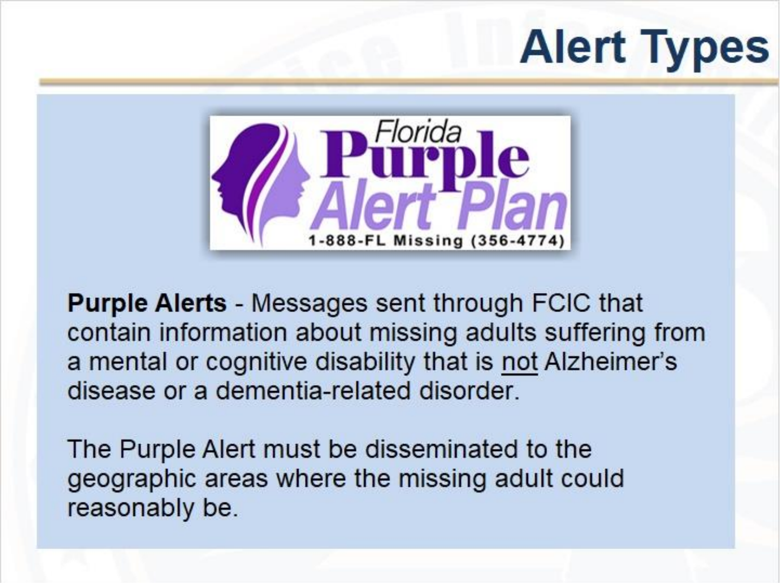
Notes:

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

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

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

1.70 Alert Types



Alert Types

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

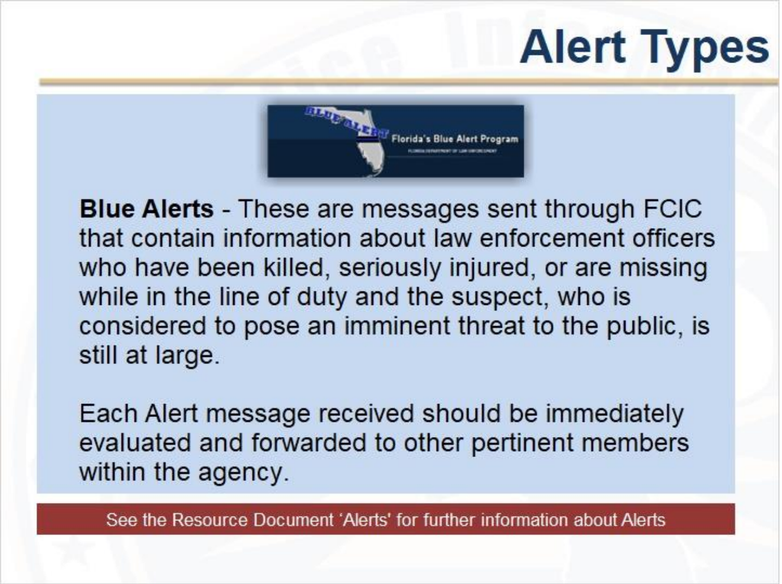
The Purple Alert must be disseminated to the geographic areas where the missing adult could reasonably be.

Notes:

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

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

1.71 Alert Types



BLUE ALERT
Florida's Blue Alert Program

Alert Types

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

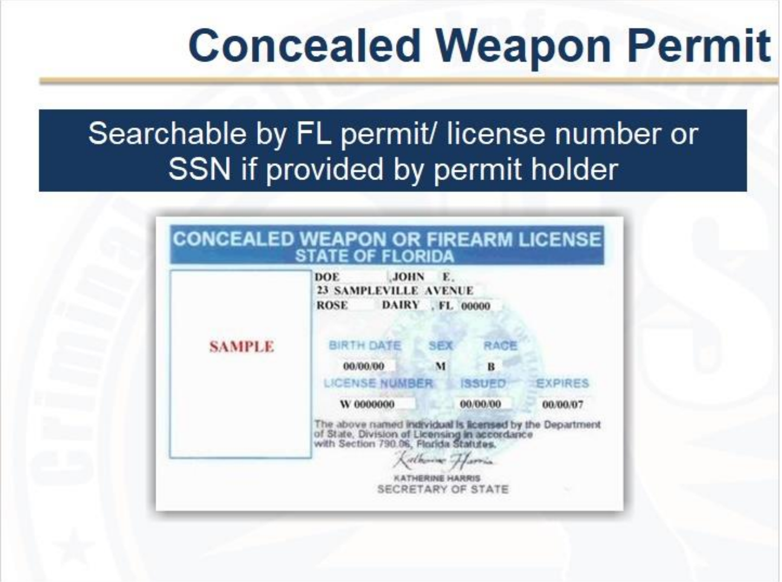
Each Alert message received should be immediately evaluated and forwarded to other pertinent members within the agency.

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

Notes:

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

1.72 Concealed Weapon Permit



Concealed Weapon Permit

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

CONCEALED WEAPON OR FIREARM LICENSE
STATE OF FLORIDA

SAMPLE

DOE JOHN E.
23 SAMPLEVILLE AVENUE
ROSE DAIRY , FL 00000

BIRTH DATE	SEX	RACE
00/00/00	M	B

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

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

Katherine Harris
KATHERINE HARRIS
SECRETARY OF STATE

Notes:

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

1.73 Concealed Weapon Permit

Concealed Weapon Permit

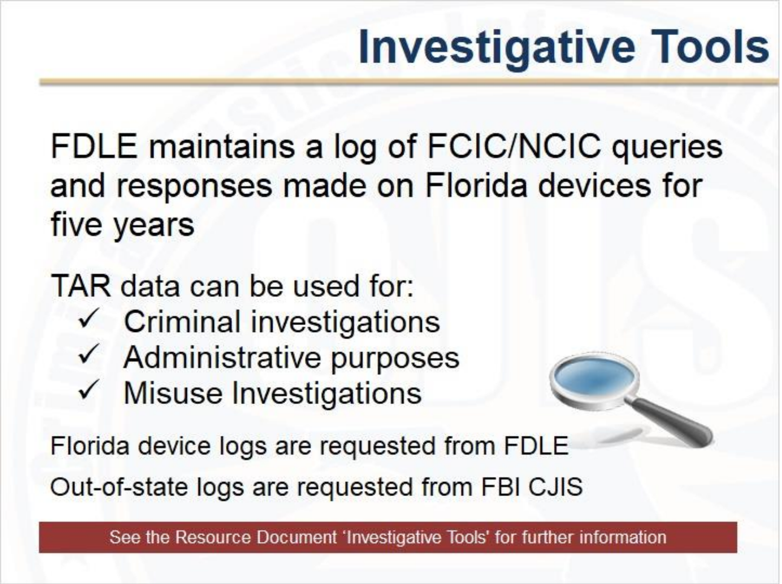
Certain states provide automated responses to Concealed Weapon Permit queries

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

Notes:

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

1.74 Investigative Tools



Investigative Tools

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

TAR data can be used for:

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

Florida device logs are requested from FDLE

Out-of-state logs are requested from FBI CJIS

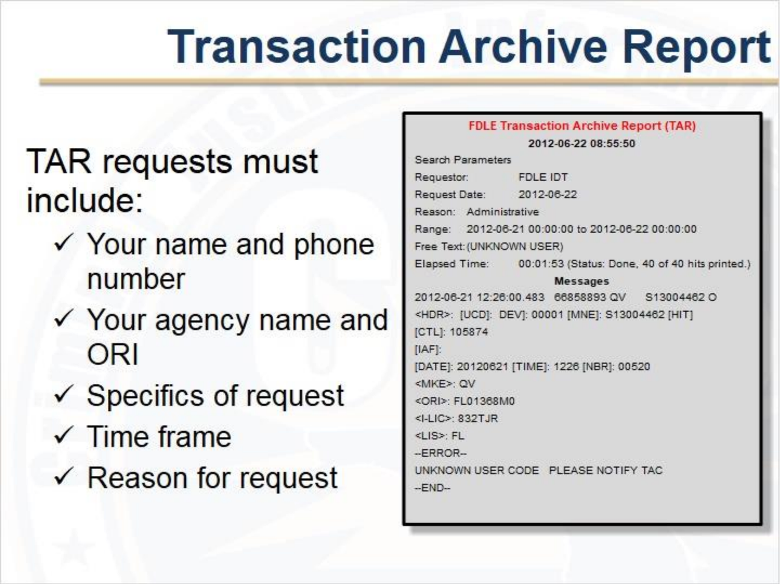
See the Resource Document 'Investigative Tools' for further information

Notes:

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

Refer to the resource document "Investigative Tools" for further information.

1.75 Transaction Archive Report (TAR)



Transaction Archive Report

TAR requests must include:

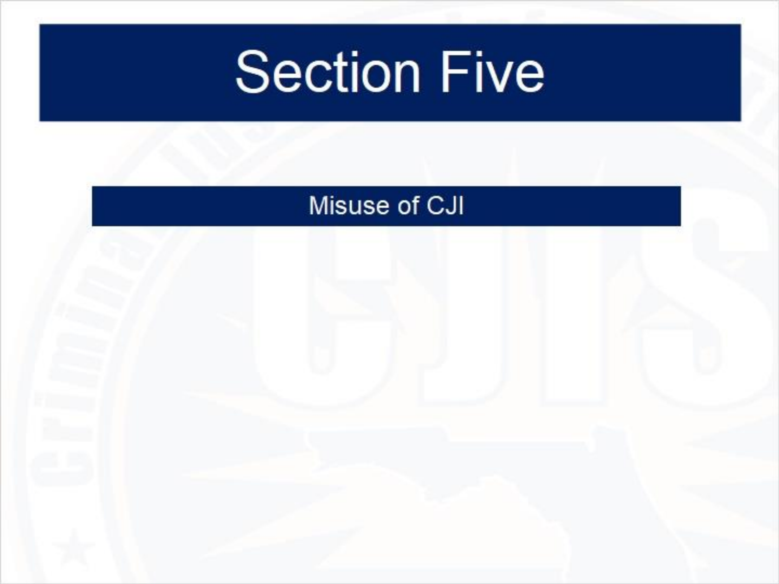
- ✓ Your name and phone number
- ✓ Your agency name and ORI
- ✓ Specifics of request
- ✓ Time frame
- ✓ Reason for request

```
FDLE Transaction Archive Report (TAR)
2012-06-22 08:55:50
Search Parameters
Requestor:          FDLE IDT
Request Date:       2012-06-22
Reason:   Administrative
Range:    2012-06-21 00:00:00 to 2012-06-22 00:00:00
Free Text:(UNKNOWN USER)
Elapsed Time:       00:01:53 (Status: Done, 40 of 40 hits printed.)
Messages
2012-06-21 12:26:00.483   66858893 QV     S13004462 O
<HDR>:  [UCD]:  DEV]: 00001 [MNE]: S13004462 [HIT]
[CTL]: 105874
[IAF]:
[DATE]: 20120621 [TIME]: 1226 [NBR]: 00520
<MKE>: QV
<ORI>: FL01368M0
<I-LIC>: 832TJR
<LIS>: FL
--ERROR--
UNKNOWN USER CODE   PLEASE NOTIFY TAC
--END--
```

Notes:

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

1.76 Section Five



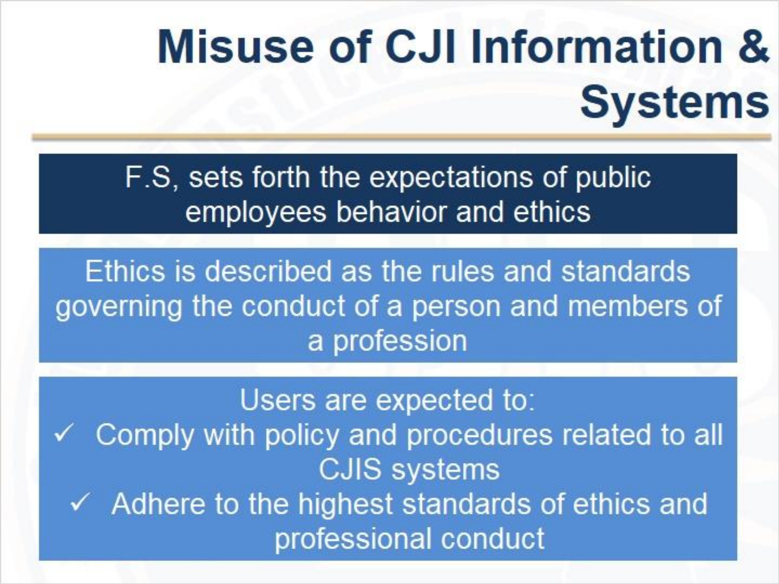
Section Five

Misuse of CJI

Notes:

Section Five 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.

1.77 Misuse of Criminal Justice Information (CJI)



Misuse of CJI Information & Systems

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

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

Users are expected to:

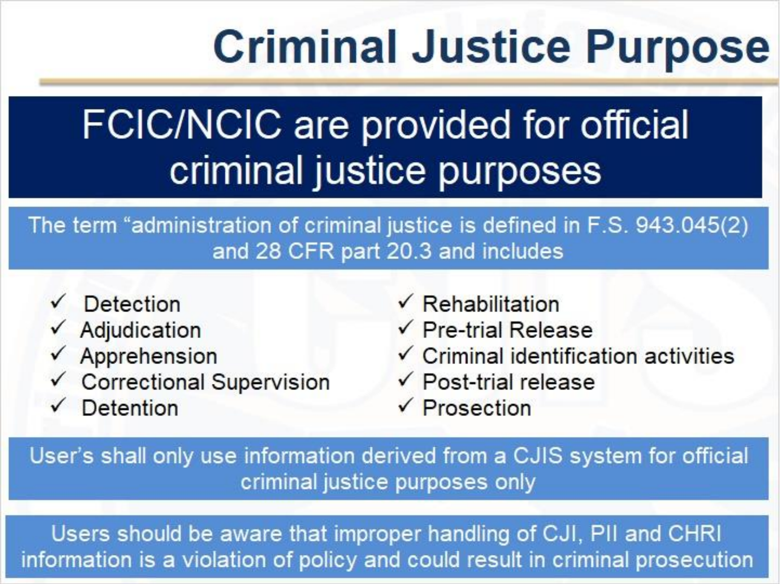
✓ Comply with policy and procedures related to all CJIS systems

✓ Adhere to the highest standards of ethics and professional conduct

Notes:

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

1.78 Common Types of Misuse



Criminal Justice Purpose

FCIC/NCIC are provided for official criminal justice purposes

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

- ✓ Detection
- ✓ Adjudication
- ✓ Apprehension
- ✓ Correctional Supervision
- ✓ Detention
- ✓ Rehabilitation
- ✓ Pre-trial Release
- ✓ Criminal identification activities
- ✓ Post-trial release
- ✓ Prosection

User’s shall only use information derived from a CJIS system for official criminal justice purposes only

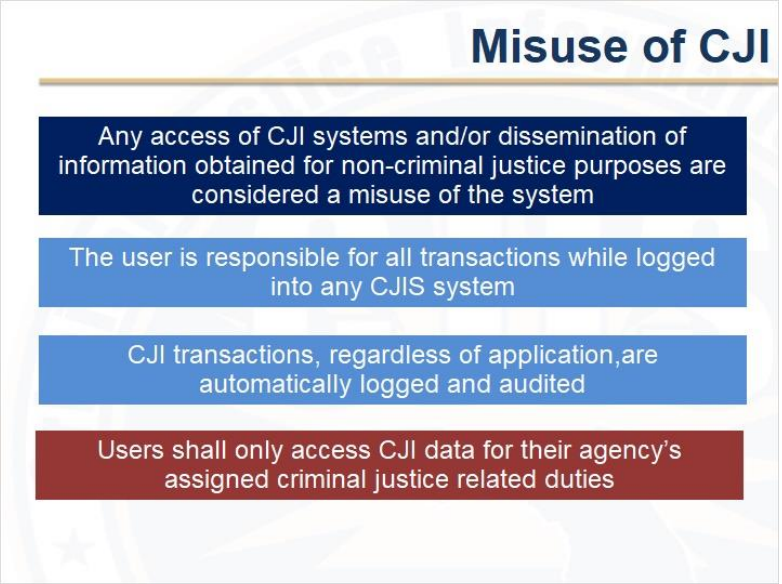
Users should be aware that improper handling of CJI, PII and CHRI information is a violation of policy and could result in criminal prosecution

Notes:

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

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

1.79 Common Types of Misuse



Misuse of CJI

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

The user is responsible for all transactions while logged into any CJIS system

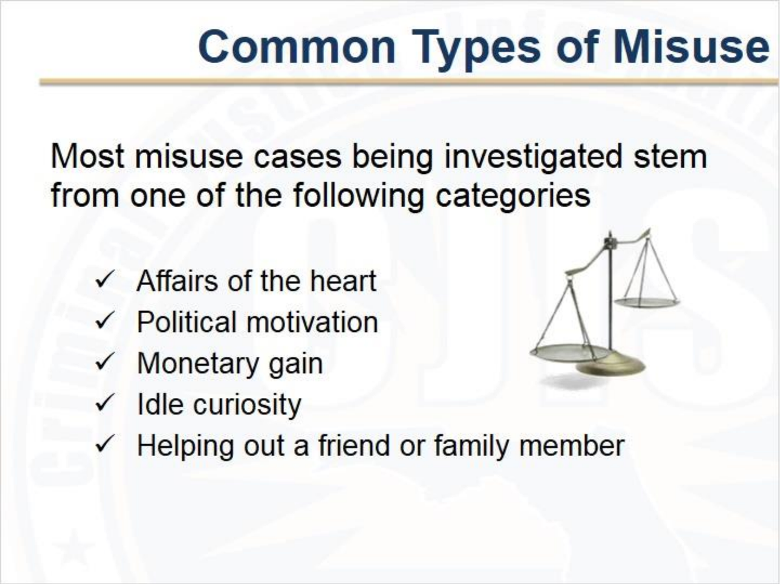
CJI transactions, regardless of application,are automatically logged and audited

Users shall only access CJI data for their agency's assigned criminal justice related duties

Notes:

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

1.80 Common Types of Misuse



Common Types of Misuse

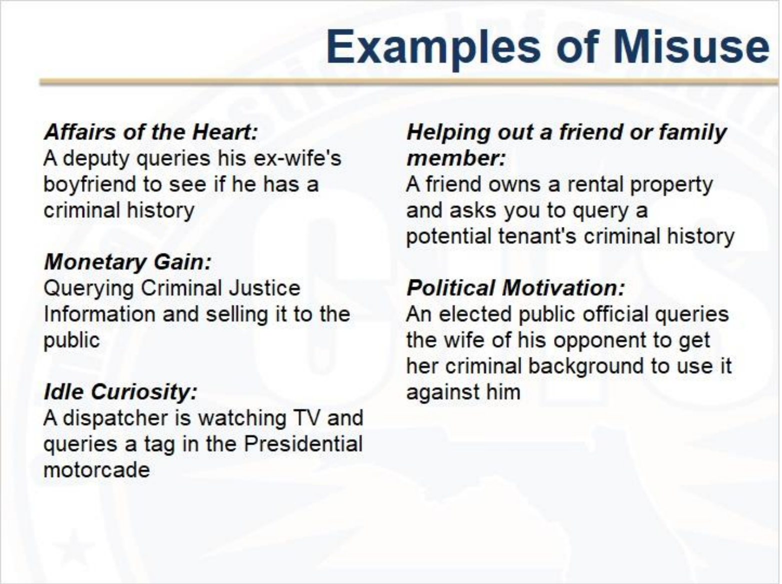
Most misuse cases being investigated stem from one of the following categories

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

Notes:

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

1.81 Examples of Misuse



Examples of Misuse

Affairs of the Heart:
A deputy queries his ex-wife's boyfriend to see if he has a criminal history

Monetary Gain:
Querying Criminal Justice Information and selling it to the public

Idle Curiosity:
A dispatcher is watching TV and queries a tag in the Presidential motorcade

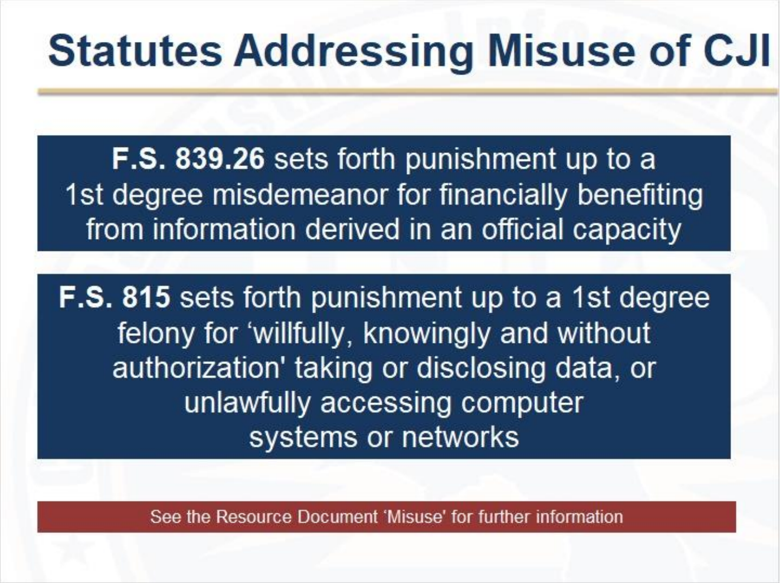
Helping out a friend or family member:
A friend owns a rental property and asks you to query a potential tenant's criminal history

Political Motivation:
An elected public official queries the wife of his opponent to get her criminal background to use it against him

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.

1.82 Statutes Addressing Misuse of CJI



Statutes Addressing Misuse of CJI

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

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

See the Resource Document 'Misuse' for further information

Notes:

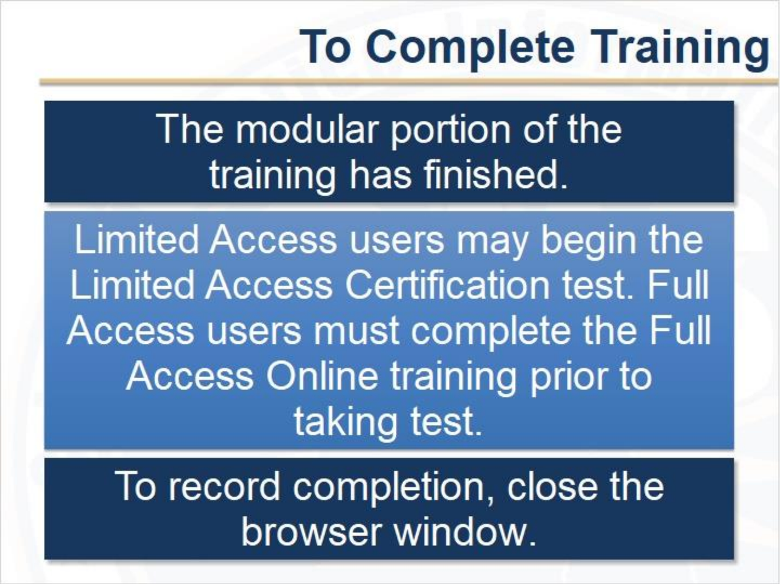
The following are Florida Statutes which address the misuse of CJI. These statutes reference both ethical and criminal violations which could be grounds for disciplinary action or termination.

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

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

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

1.83 You are Ready to Test



To Complete Training

The modular portion of the training has finished.

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

To record completion, close the browser window.

Notes:

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