# CJIS Security and Privacy Training: General User

Welcome to the CJIS Security and Privacy Training for General Users! A General User is an individual authorized to access an information system where Criminal Justice Information (CJI) is stored or processed.

The following topics will be covered:

- Introduction
- What is CJI?
- Information Security
- Roles & Responsibilities
- Access to CJIS Systems
- Security of CJIS Systems
- Conclusion

## Introduction

### Security and Privacy Training

If you have unescorted access to an area where CJI is stored or processed, you must complete Security and Privacy training before you begin your duties and once a year after that.

### Training Records

Individual training records must be retained for a minimum of three years.

## What is CJI?

The Privacy Act of 1974 established protections for individual privacy by regulating how criminal justice information could be collected, managed, used, and shared.

### Criminal Justice Information

The FBI's Criminal Justice Information Services (CJIS) division offers a range of services and provides critical data necessary for law enforcement and public safety agencies. All data provided by this division is called **Criminal Justice Information (CJI)**.

CJI can include any of the following types of data:

- **Biometric** (e.g., DNA, fingerprints)
- **Identity History** (i.e., "rap sheet")
- **Biographic** (e.g., evidence tying someone to a specific crime)
- **Property** (e.g., a gun used in a crime)
- **Case History** (e.g., stolen cars, missing persons)

The FBI CJIS Division supervises a computerized database of CJI in West Virginia called the **National Crime Information Center (NCIC)**. All information processed, stored, or transmitted to NCIC results from collaboration among the FBI and various criminal justice agencies at the federal, state, local, and tribal levels.

Another important organization in sharing criminal justice information is **Nlets**. This message switching system connects law enforcement agencies at state, local, and federal levels, enabling the exchange of critical information.

### NCIC Restricted Files

Some NCIC records have additional restrictions due to the sensitive nature of the information they contain. Examples of restricted files include Gang, Threat Screening Center, National Sex Offender Registry, Violent Person, and Supervised Release.

- **Criminal History Record Information (CHRI)** is arrest-based data collected by national and state criminal justice agencies and is sometimes referred to as "restricted data."
- The **Interstate Identification Index (III)** links FBI and participating state criminal history records into a national system. Information obtained through the III is considered CHRI and may only be accessed for authorized purposes with a documented reason.

### NCIC Non-Restricted Files

All NCIC files which cannot be classified as an NCIC Restricted File are considered **NCIC Non-Restricted Files**. Examples of non-restricted files include Boats, Guns, Missing Persons, Protection Orders, Vehicles, and Wanted Persons.

## Personally Identifiable Information

**Personally Identifiable Information (PII)** is any information that can identify a person on its own or when combined with other details, such as date of birth, gender, or race. PII should only be taken from CJI for official purposes.

***Examples of PII***

- Name
- Social security number
- Biometric records (e.g., fingerprints, retina scans)
- Driver's License or Passport number
- Personal address information (physical or email addresses)

# Information Security

Effective information handling ensures data security and compliance throughout its lifecycle.

## The Information Lifecycle

The **information lifecycle** refers to the stages that data goes through, from its creation and storage to its usage and eventual disposal. Keeping information secure during its lifecycle is essential to protect sensitive data.

- **Creation**: The inception of data, where it is secured at the point of entry
- **Storage**: Data is stored in secure, authorized locations
- **Processing**: Data is used in daily operations, with access controls and monitoring
- **Transmission:** Data is shared and transferred securely
- **Archiving**: Data no longer actively used is securely archived
- **Disposal**: Data is securely disposed of when no longer needed

Agencies must establish procedures to handle and store information securely, protecting it from unauthorized access, changes, or misuse.

# Literacy Training and Awareness

Literacy Training and Awareness means understanding risks, protecting information, and responding to security 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, follow-up literacy training can be provided in short, focused sessions. These sessions may cover new threats, policy updates, or recent incidents.

# Social Engineering and Mining

**Social engineering** is a tactic used to trick individuals into sharing information or performing actions that can compromise information systems. **Social mining** involves collecting information from user activity on social media sites to aid in future attacks.

## Message-Based Attacks

The most common form of social engineering, attackers use deceptive emails, texts, or links to trick users into revealing sensitive information or visiting malicious sites. If you cannot verify the source through a trusted channel, do not click links or share information. Report suspicious messages to your IT team.

### Key Concepts and Examples of Message-Based Attacks

- **Phishing**: Authentic-looking emails or texts designed to steal credentials or direct users to fake websites.
- **Spear Phishing**: A targeted form of phishing aimed at a specific individual or group based on their role or position
- **Quishing**: short for QR code phishing; a QR code directs users to a malicious website or triggers a malware download
- **Smishing**: short for SMS phishing; a text message with a malicious link used to steal information or install malware

## Identity Deception

Attackers fabricate a believable identity or scenario to gain the target's trust and extract information or access that would otherwise be denied.

### Key Concepts and Examples of Identity Deception

- **Pretexting**: Creating a fictional backstory or scenario to justify a request for sensitive information.
- **Impersonation**: Posing as an authority figure, co-worker, or trusted organization to make the deception convincing.
- **Social media exploitation**: Harvesting information from a target's social media profiles to craft a personalized, credible attack.
- **Fake IT Support call**: Posing as an authorized IT administrator to extract credentials or gain access to protected systems.

## False Rewards

Attackers take advantage of curiosity or self-interest by offering something appealing, such as a fix, prize, or service, that is either fake or includes a hidden security risk.

### Key Concepts and Examples of False Rewards

- **Baiting**: Luring users to a harmful website or into downloading malware through false promises or tempting offers.
- **Scareware**: Fake alarms or threat warnings that trick users into believing their system is already compromised, prompting them to click a malicious link or install harmful software.
- **Quid pro quo**: Offering a service or benefit (e.g., clearing a dispute, providing technical help) in exchange for sensitive information.

## Access Exploitation

Attackers use people's trust or distraction to get into secure areas or conversations without permission.

### Key Concepts and Examples of Access Exploitation

- **Tailgating** (piggybacking): Gaining physical access to a restricted area by following an authorized person through a secured entry, often by impersonating a delivery driver or custodian, or simply asking someone to hold the door.
- **Thread-jacking**: Inserting into a legitimate email thread to impersonate a trusted participant and gain information or access.
- **Shoulder surfing**: when someone nearby watches your screen to steal your password or other information. To prevent shoulder surfing:
  - Use a privacy screen and position your monitor so others can't see it
  - Use strong passwords and lock your device when you step away
  - Shield forms or paperwork when writing
  - Sit with your back to a wall and avoid viewing sensitive information in public areas

## Using Generative AI

Generative AI is a type of artificial intelligence that uses existing information to create new content based on user input.

***Examples of generative AI***

- Language translation
- Content creation (e.g., public relations communications, documentation)
- Safety and training enhancement (e.g., course creation, tailored coaching)
- Cybersecurity support (e.g., threat detection and analysis)
- Image generation (e.g., restoration of damaged images, face aging)

If you use a generative AI tool not approved or designed for your organization (such as ChatGPT):

- Do not enter any CJI or personal information
- Turn off chat history, if available
- Review the output carefully for errors, bias, or misleading information

# Security Incidents

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

## Incident Detection

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

***Examples of incident indicators***

- New user accounts are created without following standard procedures
- Sudden high activity on an inactive or low-activity account
- New files with unusual names appear
- Unexpected data changes or removal of data
- Unexplained poor system performance or system crashes

## Incident Reporting

Report any incidents or unusual activity to your agency contact, personnel with security responsibilities, 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

The following information should be included in the incident report:

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

Users should have access to automated resources for incident response, such as help desks and ticketing systems, to assist with handling and reporting incidents.

## Audit Record Review, Analysis, & Reporting

Agencies must designate a person or role to manage audit record review and reporting. System audit records must be analyzed ***weekly*** for unusual activity and share their findings with relevant officials.

After confirming the incident, notify the CJIS Systems Officer (CSO), State Identification Bureau (SIB) Chief, or Interface Agency Official. Also, share incident details with the supplier of the related products or services involved in the incident.

## Incident Response

Agencies must maintain an incident response policy that is reviewed every year and anytime there is a security incident involving unauthorized access to CJI or related systems.

All users with access to unencrypted CJI must be trained on this policy and the steps they must follow after an incident has occurred.

## Incident Response Training

Incident response training should teach users how to recognize and report suspicious activity. The training should be based on each user's job role and completed before system access. It must also be updated and retaken every year.

***Examples of training according to a user's assigned role***

| User Role | Type of Training |
|---|---|
| Average User | Needs to know how to recognize an incident and who to contact |
| System Administrator | Needs additional training on how to handle incidents |
| Incident Responder | May need more specific training on forensics, data collection techniques, reporting, system recovery, and system restoration |

## Incident Response Testing

The system's incident response capabilities must be tested every year using exercises or simulations. Testing should correspond with other related capabilities, such as disaster recovery and emergency response.

## Incident Response Life Cycle

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

| |
|---|
| **Preparation**<br>Training a response team and gathering the tools needed to respond to incidents. |
| **Detection and Analysis**<br>Finding the cause of an incident and understanding its impact. |
| **Remediation and Recovery**<br>Stopping the attack, removing the threat, fixing weaknesses, and restoring systems. |
| **Post-Incident Activity**<br>Reviewing what happened and using lessons learned to improve future responses. |

These phases help organizations respond quickly, limit damage, and improve future incident response. Automated tools, like online incident management systems, should be used to help manage and support the incident response process.

***Example of the incident response life cycle***

The following scenario illustrates how the incident response lifecycle phases work together in a real-world situation:

**Preparation**: A police department implemented security software and trained all staff to spot suspicious activity and report it right away.

**Detection and Analysis**: A staff member noticed her computer acting strangely, reported it immediately, and the IT department confirmed that it was caused by a phishing email.

**Remediation and Recovery**: The infected computer was taken off the network, the virus was removed, and the computer was restored.

**Post-Incident Review**: The investigation showed no sensitive data was affected, and the agency improved email filters and trained staff how to recognize phishing emails.

# Roles & Responsibilities

All users with access to CJI have specific responsibilities based on their role and level of system access.

## Agency Roles and Responsibilities

Agencies must protect CJI by following the technical and procedural requirements outlined in the CJIS Security Policy. Agencies are also required to develop and maintain information security policies and procedures, including penalties for CJI misuse.

Agency personnel responsible for CJI include:

- **CJIS Systems Agency (CSA)** is 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 government agency that administers criminal justice according to laws or executive orders. Examples of criminal justice agencies 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 related to CJI 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 may access CJI include a 911 communications center providing dispatch services for a criminal justice agency, a bank running a background check on potential employees, and a county school board utilizing criminal history records for employee hiring decisions.
- **Organizational Personnel with Information Security Responsibilities** are agency personnel responsible for ensuring the confidentiality, integrity, and availability of CJI and the agency's compliance with the CJIS Security Policy. Examples of organizational personnel with information security responsibilities are Local Agency Security Officer (LASO), Authorized Recipient Security Officer (ARSO), Agency Head, Chief Information Officer (CIO), Auditor, Incident Response Coordinator or Analyst, System Administrator, and Emergency Response Coordinator.

  **Key security responsibilities include:**

  - Monitoring access to approved hardware, software, and firmware
  - Documenting agency connections to the state system
  - Managing personnel security screening procedures

- Ensuring security measures are properly implemented and functioning
- Ensuring policy compliance and reporting security incidents to the CSA

### Information Exchange

Sometimes your agency's system needs to share Criminal Justice Information (CJI) with another agency's system, for example when two agencies work together on a case or share access to the same database.

Before agencies share this information, they must have a signed agreement. The agreement should include information such as:

- Who is allowed to access the shared information
- What the receiving agency can and can't do with it
- Security requirements both agencies must follow
- How the agencies will handle audits and reporting

## Individual User Responsibilities

Individuals are responsible for their own behavior regarding CJI. Individual user responsibilities include the following:

- 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 documented terms and conditions for such systems)
- Do not use public computers to access, process, store, or transmit CJI
- Never use CJI for personal use or gain

## Top 5 Daily Security Tips

1. Use a unique user ID and password.
2. Be accountable for all actions taken when accessing or using CJI.
3. Never share passwords or leave them in visible locations.
4. Lock your computer or use a password-protected screensaver when stepping away; .
5. Log out of the system at the end of your shift or before another user accesses the system.

## Contractor/Vendor Responsibilities

Private contractors who perform criminal justice functions must meet the same training and certification requirements as governmental agencies performing a similar function. They are also subject to the same audits as local agencies.

### CJIS Security Addendum

All private contractors who perform criminal justice functions must sign the **CJIS Security Addendum**. This is an addendum to the agreement between a criminal justice agency and a private contractor which specifies the contractor's scope and purpose for providing services.

The Security Addendum includes the following security provisions for contractors:

- Authorizes access to CJI
- Ensures information security aligns with CJIS Security Policy and related regulations
- Limits the use of information to the purpose for which it is provided

- Provides for sanctions

# Access to CJIS Systems

## Access, Use, and Dissemination

The CJIS Security Policy sets the minimum standard for accessing, using, and sharing CJI. Local policies can **increase** restrictions but should not lower them.

### Proper Access, Use, and Dissemination of CHRI, III, and NCIC Restricted Files Information

CHRI, III, and NCIC restricted files must only be accessed for authorized purposes under federal law. CHRI received from the III system must be used for the **same** authorized purpose for which it was requested.

Information may be shared with another agency if they are an Authorized Recipient being serviced by the original agency, or if they are handling employment or appointment decisions for criminal justice applicants.

***Example of authorized purpose and usage of CHRI***

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.*

### Noncriminal Justice Access and Use of CHRI

Noncriminal Justice agencies may access CHRI if the following qualifications are met:

- Must be authorized to receive it by a federal statute, executive order, or an approved state statute
- Using the information to support employment suitability, licensing decisions, immigration processes, and national security clearances.
- Has full consent from the person being checked

For more information on the proper access, use, and dissemination of CHRI, III, and NCIC Restricted Files, refer to Title 28, Part 20, CFR and the NCIC Operating Manual.

### Proper Access, Use, and Dissemination of NCIC Non-Restricted Files Information

NCIC non-restricted information may be accessed and used for any approved purpose related to the agency's official duties. The agency may share this information with other government agencies or private organizations if the law allows and the use fits their official duties.

Non-law-enforcement use is allowed only in limited situations:

- Requests should be reasonable and not involve large amounts of data
- The information may only be used to check person or property status, such as whether a person is wanted or a vehicle is stolen

- It must not be used for research, marketing, or business purposes. Agencies may charge a small fee to cover administrative costs
- If restricted information is included, it may only be shared for law-enforcement purposes

### Methods of Dissemination

Each communication method requires different safeguards to protect CJI.

| Method | Guidance / Requirements |
|---|---|
| **Phone / Radio** | **Voice transmission of CJI should be limited.** Share details only when immediately needed for an investigation or when officer or public safety is at risk. |
| **Email** | **May be used if proper protections are in place.** The email service must meet CJI encryption, authentication, spam, and antivirus requirements. Always verify recipient authorization before sending CJI. |
| **Fax** | **May be used only if both agencies are authorized and have an ORI.** Encryption for CJI-in-transit is required unless using a standard telephone line. Always verify the receiving agency's authenticity before sending. |
| **Text** | **Default text applications must not be used.** Apps that do not require login every time are not secure. Only approved text applications with proper encryption and authentication may be used. |

### Access, Use, and Dissemination Penalties

Unauthorized access, use, or sharing of CJI, including CHRI, NCIC Restricted, and NCIC Non-Restricted Files information, is a serious violation and may result in the following penalties:

- **Criminal prosecution**
- **Termination of employment**

### Personnel Sanctions

Agencies must implement a formal disciplinary process for any personnel who fail to comply with the security policies and procedures.

Once the sanctions process has been initiated, personnel with information security responsibilities and other administrators with account management responsibilities must be notified within ***24 hours***.

## Managing Access

**Access Control** is the regulation of permissions regarding who can access specific resources and information within an organization.

### Access Control Criteria

Authorized access to the information system should be based on:

- Valid privileges
- Intended system usage
- Account attributes associated with the user, such as certification indicators or sworn law enforcement designation

*Note: See AC-2(d)(3) in the CJIS Security Policy for a full list of possible attributes*

### Least Privilege

The principle of **least privilege** means giving individuals only the access they need to perform their jobs.

### Separation of Duties

The principle of **separation of duties** means dividing roles so that different people handle different administrative tasks. For instance, personnel who can assign user access should not have access to audit logs that show account activities.

## Personnel Security

All personnel with unescorted access to CJI must be screened and held accountable for maintaining security and privacy standards.

The minimum requirements for screening individuals who need access to CJI include:

- Job descriptions must include security and privacy roles and responsibilities
- State of residency and national fingerprint-based records checks
- Users must sign an access agreement before being granted system access
- The granting agency must maintain a list of personnel who have authorized access to CJI

### Transfer

When an employee changes positions within the agency, their system and facility access must be reviewed and updated.

### Termination

When an employee leaves agency, all agency property must be collected, and their system access must be disabled. An exit interview should be conducted to remind them not to share CJI or personal information.

## Access Enforcement

Access to CJIS systems must be enforced at both the system level and the application and service level to ensure comprehensive security and privacy protection.

### Individual Access

Individuals should have the ability to access their personally identifiable information (PII) through automated tools or request forms. This access allows them to understand how their PII is used and verify its accuracy.

### Publicly Accessible Content

Publicly accessible content is information managed by the organization that anyone can access without logging in. This includes everything on the organization's public website. It is important to review this content every three months to remove any nonpublic information that might be included by mistake.

The organization's policy should clearly state the rules for sharing information on public websites, forums, and social media.

# Physical Access Control

Access to secure locations must be controlled by verifying authorizations before allowing access.

## Physical Access Authorizations

Agencies must keep a list of authorized individuals and provide ID badges or credentials to control access to secure areas.

## Physical Controls and Access Management.

Physical controls secure CJI areas by limiting visibility and ensuring only authorized access.

### Physical Access Devices

Use physical security devices like locks and biometric readers to stop unauthorized access to secure areas. Change locks or codes if keys are lost or if users with access leave or are no longer authorized.

### Monitoring Physical Access

Monitor access to secure locations to identify and address security issues. This can include using guards, video cameras, and sensors.

### Access Control for Output Devices

Output devices such as monitors, printers, scanners, fax machines, and copiers can put CJI at risk if unauthorized individuals can view or access them. Protect these devices by using privacy screens, securing them in restricted areas, and retrieving printed or faxed CJI immediately.

### Visitor Access Records

Always escort visitors and monitor all activities in secure areas. Visitor access records must be kept for one year and include the following:

- Visitor's name and organization
- Visitor's signature
- Forms of ID
- Date of access
- Entry and exit times
- Purpose of visit
- Name of person being visited

## Controlled Areas

If an agency cannot fully meet the physical access control requirements, a specific area or container must be designated as a **controlled area** for daily access or storage of CJI. It is the responsibility of all personnel to help keep controlled areas secure.

The controlled area should have the following security measures:

- Store hard copies containing CJI in a way that prevents unauthorized access, such as locked file cabinets.
- Encrypt stored digital devices using the requirements for CJI-at-rest
- Position information system devices and documents containing CJI in a way to prevent unauthorized users from viewing them. For example, if a computer faces outside the secure area, it is not secure.

- Limit access to the secure area only to personnel authorized by the agency to access CJI.
- Lock the area, room, or storage container when unattended

## System Access Control

Access to CJIS systems must be strictly controlled to ensure only authorized users can read, write, or delete data.

### User Session Controls

Implementing user session controls, such as automatic device lock and session termination, can reduce the risk of unauthorized access.

### System Use Notification

A notification must be presented to users before they access the system which includes the following information:

- The user is accessing a restricted information system.
- By using the system, the user agrees to possible monitoring and recording of activities.
- Unauthorized use is prohibited and may lead to criminal and/or civil penalties

### Device Lock

All devices accessing the system must automatically lock within 30 minutes of being idle, or sooner for mobile devices.

*Note: Device locks serve as a temporary security measure and should not replace the practice of logging out of the information system.*

### Session Termination

When a user logs out, their session should end automatically. Sessions may also be set to end after certain events, such as a password change, system restart, or at a specific time.

### Unsuccessful Login Attempts

User accounts should be automatically locked after repeated unsuccessful login attempts. Users must contact their administrator to regain access.

## Media Protection

**Media** refers to the physical and digital items used to store, process, or share data. Media that contains CJI must be accessed, stored, and disposed of safely to prevent unauthorized access or exposure.

***Examples of physical media***

- Paper
- Microfilm
- Physical photographs (such as crime scene photos or mugshots)

***Examples of digital media***

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

- Notebook computers

### Media Access

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

#### *Example of Physical Media Access Restrictions*

An example of restricting access to physical media would be to implement a policy that permits only authorized users to access hard copies of case file information stored in a locked filing cabinet.

#### *Example of Digital Media Access Restrictions*

An example of restricting access to digital media would be to implement a policy that permits only the system development team to access a flash drive containing system design specifications.

### Media Storage

All media must be stored in a physically secure location or controlled area. If physical security is not possible, CJI on digital media should be encrypted to protect it. Procedures must be in place to allow users to check out and return media properly, ensuring accountability and protecting the security of the information at all times.

### Media Disposal

Media must be sanitized and destroyed using formal, documented procedures. Media disposal should be witnessed or carried out by authorized personnel to minimize the risk of compromising information.

### Physical Media Disposal

When hard copies no longer need to be retained, physical media must be destroyed by **shredding** or **incineration**.

### Digital Media Disposal

Digital media should be disposed of using the preferred methods listed below, in order of priority:

1. Digital media must be sanitized prior to disposal (before reusing or transferring to a non-criminal justice entity).
2. Physical destruction is recommended for disposal of digital media.
3. If physical destruction is not possible, it must be overwritten at least three times to prevent unauthorized access to previously stored data.

# Security of CJIS Systems

## Security Threats & Vulnerabilities

A security **threat** is any situation, event, or threat actor that can harm an information system by altering, disclosing, or destroying data. A security **vulnerability** is any weakness in security procedures, technical controls, physical controls, or other safeguards that could be exploited by a threat.

### How Security Threats Start

- **Threat Actor:** A person or group that deliberately compromises systems or data. Threat actors can include cybercriminals, hackers, and even insiders. They are often motivated by money, beliefs, personal satisfaction, or discontent.
- **Insider Threat:** An agency's own personnel can be one of its greatest security risks. Insider threat may be signaled by prolonged job dissatisfaction, hostile behavior, or attempts to access information without proper authorization.

***Examples of threats***

- **Natural:** lightning, heat, or water
- **Intentional:** a threat actor intending to cause harm.
- **Unintentional:** a user accidentally deleting a critical file

***Examples of vulnerabilities***

- **Physical:** using an information system in a non-secure location
- **Natural:** connecting your computer to a power source without a surge protector or backup power supply
- **Hardware:** connecting an information system to the internet without a firewall
- **Software:** not keeping your computer's operating system updated

Information systems in a network are especially vulnerable because each connected device could have weaknesses. Once an attacker gains access to one device, they can move between systems, increasing the risk of widespread damage.

## Systems Security

Systems Security refers to measures taken to protect an information system from unauthorized access or misuse.

### Data Protection Methods

#### Cryptographic Protection

**Cryptographic protection** helps keep sensitive information secure by using approved tools, such as encryption. Encryption changes readable information into a protected form so only authorized people or systems with the correct key can read it.

#### Protection of Information at Rest

**Information at rest** is CJI that is stored on a device or service, such as a laptop, external drive, or approved cloud storage. This is different from **information in transit**, which is CJI being sent from one location to another. If CJI is stored outside a physically secure location, it must be encrypted. Only use storage locations approved by your agency.

#### Malicious Code Protection

**Malicious code protection** prevents harmful software, called *malware*, from damaging information systems. Common types of malware include viruses, worms, adware, and ransomware.

Malicious code protection should include:

- Virus protection to find and remove malware on all network devices, including computers, servers, and mobile devices.
- **For all systems with internet access:** automatic software updates

- **For all systems *not* connected to the internet:** local procedures to keep malicious code protection current

### Spam Protection

**Spam protection** helps stop unwanted or unsafe messages from reaching users. It should be used on email systems and other approved messaging tools to reduce the risk of harmful links, unsafe attachments, and other suspicious content.

## Wireless Access

Wireless access has special risks, so extra care is needed to protect sensitive data. Clear guidelines for wireless use must be clearly defined in writing before users are allowed to connect to the system wirelessly.

### Types of Wireless Connections

| Wireless Connection | What it is | Risks | Safety Tips |
|---|---|---|---|
| Bluetooth | Bluetooth lets nearby devices connect wirelessly, such as phones, laptops, keyboards, and headsets. | • Others may listen in on the connection<br>• Attackers can take control of the device | • Use strong passwords for pairing devices<br>• Reject and report unknown connection requests<br>• Turn off Bluetooth when not in use |
| Wi-Fi | Wi-Fi allows devices like laptops, phones, and printers to connect to the Internet wirelessly. | • Unauthorized access through wireless networks<br>• Malware entering through connected devices | • Keep a list of all wireless access points<br>• Place access points in secure areas<br>• Regularly check security settings, such as encryption and firewalls |
| Mobile Hotspot | A mobile hotspot lets a phone or tablet share its Internet connection with other devices. | • Data can be intercepted<br>• Network name may reveal agency or device details<br>• Malware can spread to other devices | • Use encryption<br>• Change the default hotspot name<br>• Allow only agency-approved devices to connect |

### Protecting Wireless Devices

In addition to the safety tips for specific wireless connection types, follow these general practices to help reduce security risks to wireless devices.

- Keep device operating system updated
- Use multi-factor authentication and device login security
- Encrypt all CJI on the device and clear stored data after use
- Use personal firewalls and antivirus software

# Mobile Device Security

## Cellular Devices

A **cellular device** is any device that uses cellular technology, such as smartphones, tablets, and PDAs. These devices face higher security risks because they are small, easy to carry, and connect to many services.

Common risks to cellular devices include:

- Loss or theft
- Unauthorized access
- Malware and spam
- Electronic tracking

## Mobile Device Management (MDM)

Mobile Device Management (MDM) is software that helps system administrators manage user device settings, applications, and security.

MDM must include these security features for any devices that access CJIS Systems:

- Lock or erase devices remotely
- Enforce security rules like encryption
- Find lost devices
- Detect unsafe apps
- Block devices that are not updated or secure

# Use of External Systems

An external system is any system or device your agency doesn't own or control, like a personal phone or laptop, a public computer, or a system belonging to another organization. Only use an external system to access, process, store, or transmit CJI if your agency has specifically approved it for that purpose.

## Remote Access

**Remote access** allows users to connect to agency systems from outside the agency network, such as when working from home or traveling. To help keep information secure, remote access should be limited to agency-approved tools and methods.

## Personal Devices

Do not use personal devices to handle CJI unless your agency has approved rules in place.

## Public Computers

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

***Examples of places where public computers can be found***

- Hotel business centers
- Convention centers
- Public libraries
- Public kiosks

### Portable Storage Devices

Only use storage devices, such as USB drives, that have been issued or approved by your agency and connect them only to authorized systems. CJI should not be stored on personal devices because they may not meet required security and encryption standards.

### Collaboration Tools Security

Collaboration tools include apps and devices used for meetings and communication, such as cameras, microphones, and platforms like Teams, Zoom, and Webex. These tools create security risks if not used carefully.

Follow these best practices to keep information secure during collaborations:

- Hide sensitive information before sharing your screen
- Turn off screen sharing before entering user IDs or passwords
- Do not allow remote control of devices
- Check indicator lights to confirm devices are off when not in use

## Identification and Authentication (Organizational Users)

Any individual who accesses, processes, stores, or transmits Criminal Justice Information (CJI) must be uniquely identified and authenticated.

### Identification

**Identification** is a way to uniquely represent a user, machine, or entity in an information system.

***Examples of Identifiers***

- **Personal Identifier** – User ID, email address
- **Agency Identifier** – Originating Agency Identifier (ORI)
- **Device Identifier** – MAC address, device-unique token

### Authentication

**Authentication** is the process of verifying the identity of a user before allowing access to the information system.

### Multi-Factor Authentication (MFA)

Multi-factor authentication (MFA) is the use of two or more different factors for authentication. This process increases confidence that the identity of the user is legitimate.

Authentication factors include:

- **Something you know** (a password or PIN)
- **Something you have** (a one-time password generated by an authenticator application)
- **Something you are** (a fingerprint or facial recognition).

### Memorized Secret Authenticators and Verifiers

Requirements for user-chosen passwords include:

- Must be at least 8 characters, longer is better
- Can include spaces, so a full passphrase is allowed and encouraged
- Must not be a standalone dictionary word; dictionary words may be used in a passphrase
- Must not be repetitive or sequential characters (e.g., 'aaaaaa', '1234abcd')

- Must not be context-specific words, such as the name of the service, username, or title
- Should not be reused across multiple accounts

**Password examples for user-chosen passwords:**

| BAD Password | Reason |
|---|---|
| 3kidz | Too short |
| Elephant | Standalone dictionary word |
| 87654321 | Sequential characters |
| Admin2024 | Context-specific |

# Conclusion

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

**Completion of this training does not guarantee certification.** Keep reading to find out your next steps and make sure you meet all the certification requirements.

## 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, you may also need to complete additional training or pass a test to be considered certified.

# Limited Access 2026V3

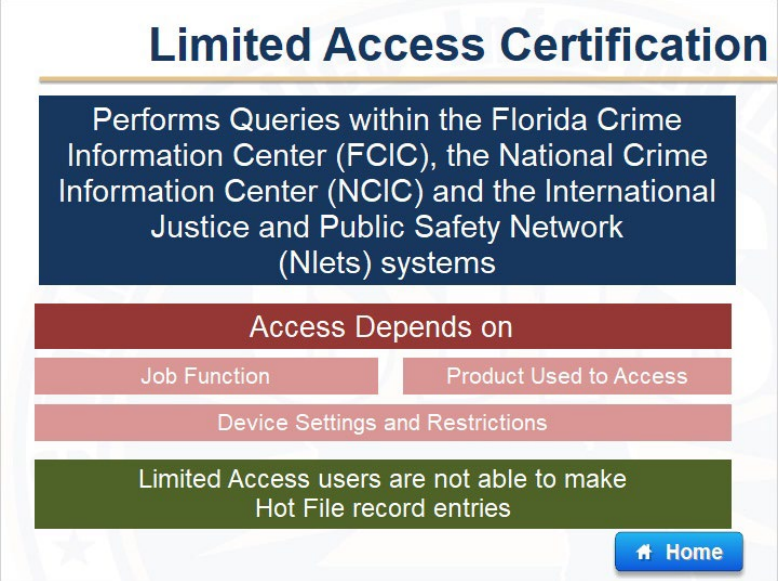
## 1. Limited Access 2026v3

### *1.1 Home Page*


**Notes:**

Welcome to the Florida Department of Law Enforcement (FDLE) Criminal Justice Information Services (CJIS) Limited Access Certification Course. To begin training, select the first topic on the left. As each topic is completed click on the home button too return to this page where you will select the next topic. Please allot at least one hour of uninterrupted time to complete this training. If training must be stopped, please exit the browser window to bookmark where you have left off. You will be able to return and continue your training. Once training is started, it must be completed within 14 days of the initial start time.

## *1.2 Introduction*

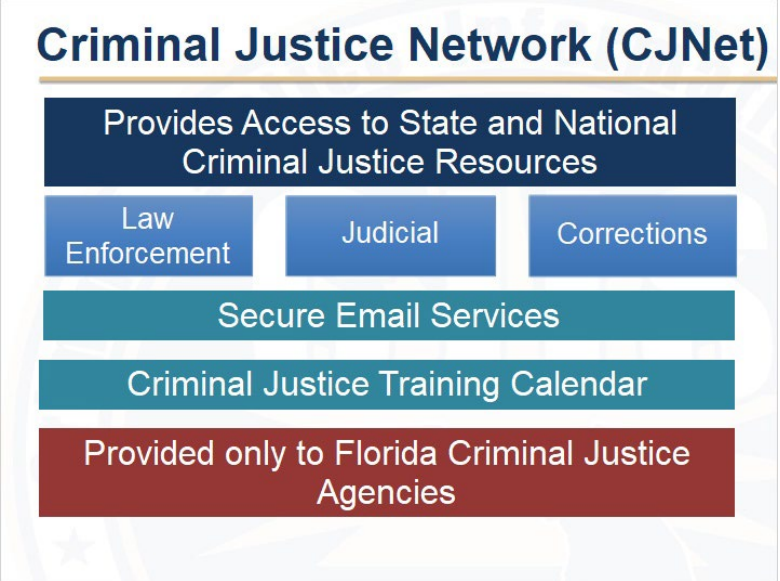



**Notes:**

A Limited Access user is defined as an operator at any 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. Select the home button to return to the main screen.

## *1.3 Criminal Justice Network (CJNet)*




**Notes:**

The Florida Criminal Justice Network, otherwise known as the CJNet, is maintained by FDLE and provides access to state and national criminal justice resources relating to law enforcement, judicial, and correctional information. 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 agencies.

## *1.4 National Crime Information Center (NCIC)*


**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.

## *1.5 CPIC*


**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.

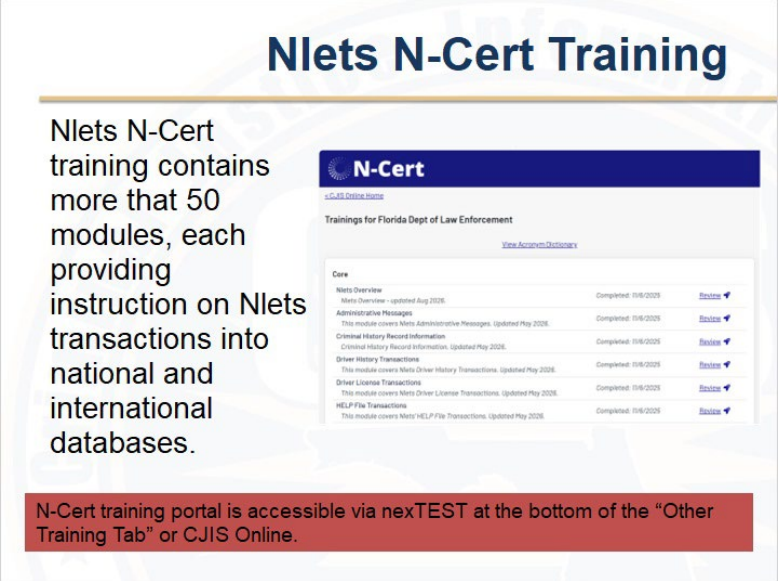
- WQ for Persons
- VQ for Vehicles
- CAQ for Articles
- CGQ for Guns
- CSQ for Securities and
- CBQ for Boats

## *1.6 International Justice and Public Safety Network (Nlets)*


**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 related information over a high-speed message switching system. Nlets supports inquiries into each state's motor vehicle, driver's license/history, and criminal history files, as well as other relevant databases. For additional information see the resource document “Nlets Resources Companion Document” or www.Nelts.org. For training see the Nlets N-Cert Portal on nexTEST or CJIS online.

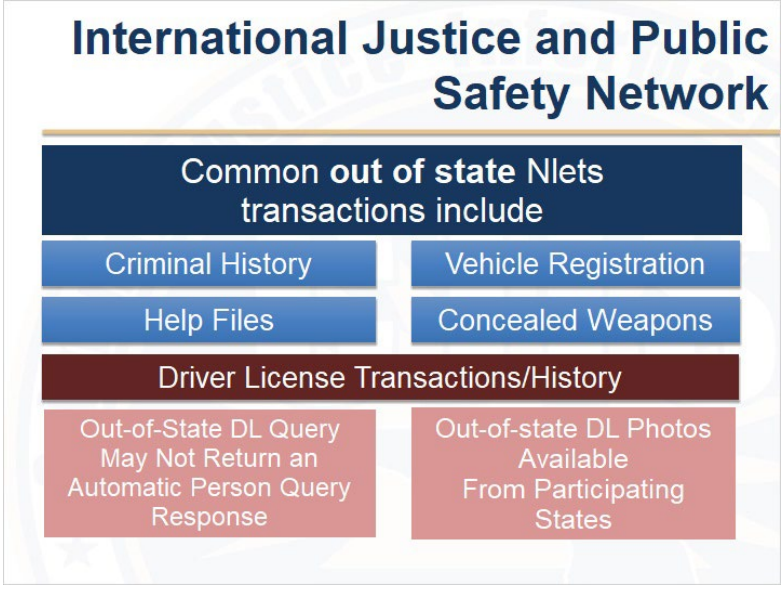
## *1.7 Nlets N-Cert Training*




**Notes:**

- N-Cert training contains more that 50 modules, each providing instruction on different Nlets transactions into national and international databases.
- N-Cert training is available via nexTEST or CJIS Online.

## *1.8 Nlets*



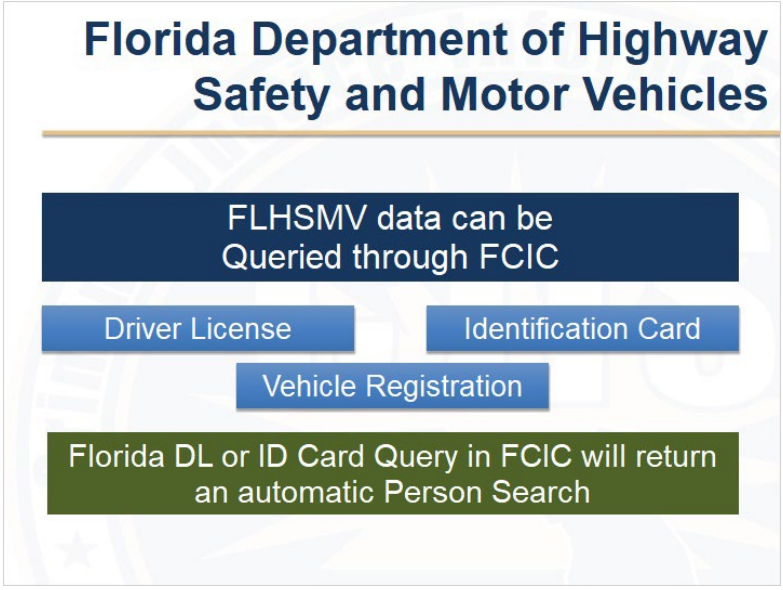

**Notes:**

The most commonly used Nlets queries for national information are: Criminal History, Vehicle Registration, Help Files, Concealed Weapons, and Driver License Transactions/History. 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.

Additionally, 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 with specific vehicle details such as vehicle type, make, model, year and more.

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

### *1.9 DHSMV*

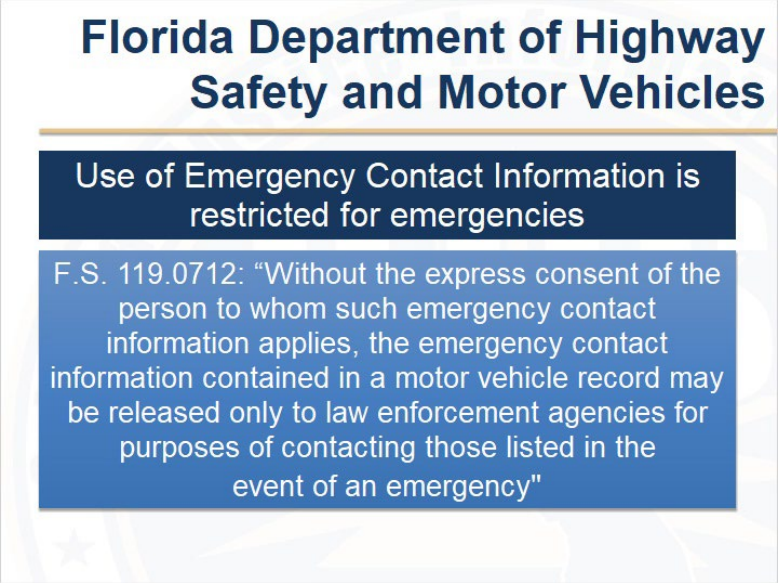



**Notes:**

Users may query FLHSMV data through FCIC, and receive responses from FLHSMV, FCIC, NCIC, and perhaps Nlets, depending upon search criteria used. A Florida FLHSMV response will be received when a Florida driver license, identification card and vehicle registration query is made using FCIC. A 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.

### *1.10 DHSMV*

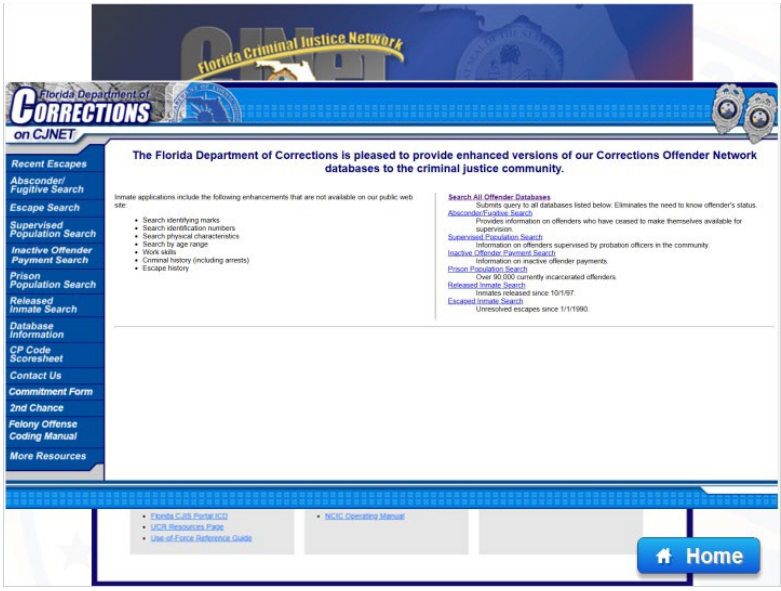



**Notes:**

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."*

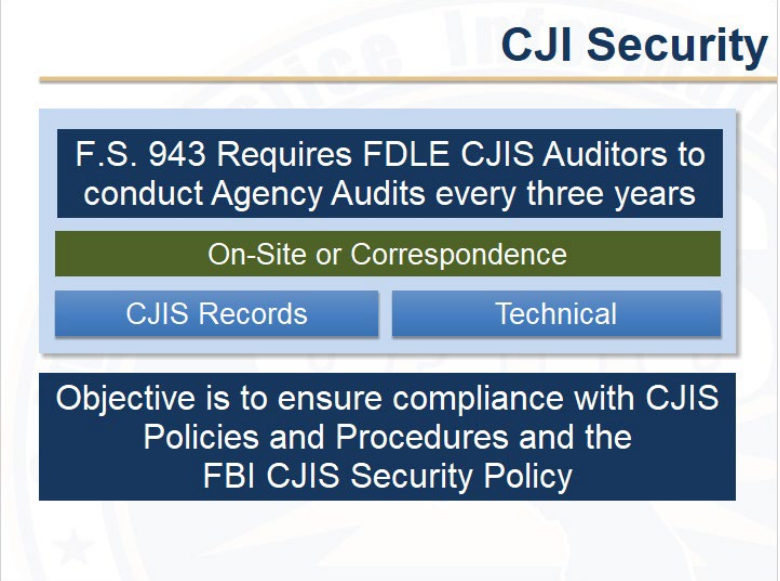
## *1.11 CJNet*




**Notes:**

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 access 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. Select the home button to return to the main screen.

## *1.12 CJIS Compliance*



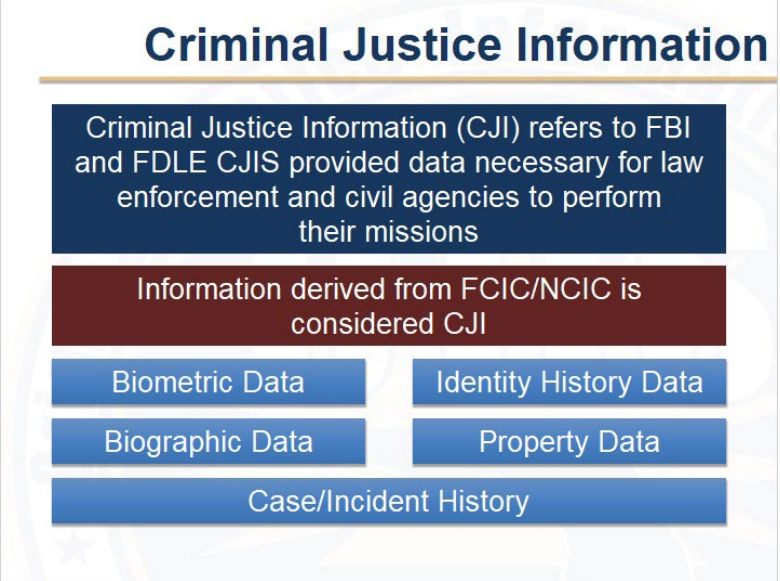

**Notes:**

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

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

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

## *1.13 Criminal Justice Information*




**Notes:**

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

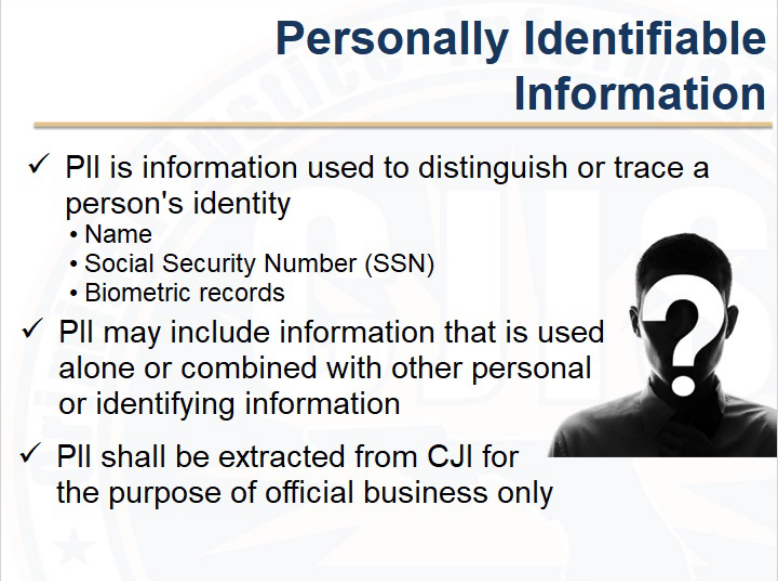
CJI includes biometric data which is used to uniquely identify individuals from within a population; Identity History is textual data that corresponds with a subject's biometric data, providing history of criminal and/or civil events; Biographic Data is information about subjects associated with a unique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

## *1.14 Florida Crime Information Center (FCIC)*


**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 for Florida concealed permits only and is provided only to law enforcement agencies.

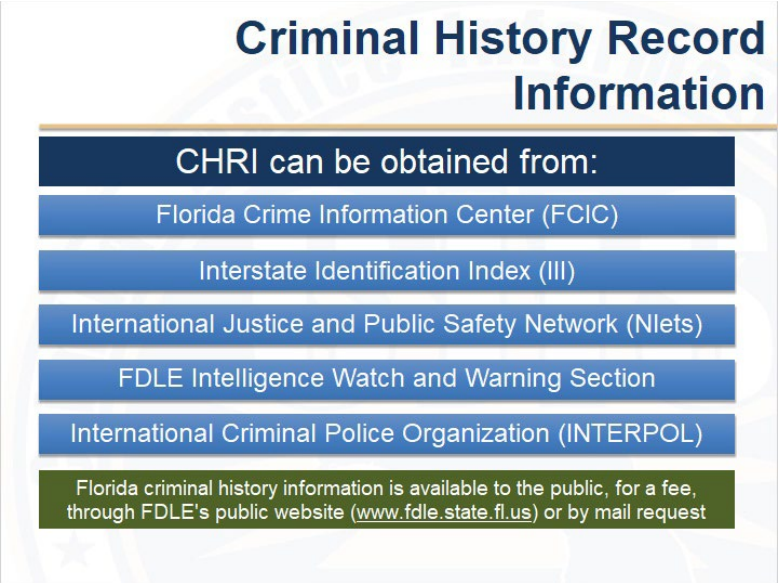
## *1.15 Personally Identifiable Information*




**Notes:**

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

## *1.16 Criminal History Record Information (CHRI)*



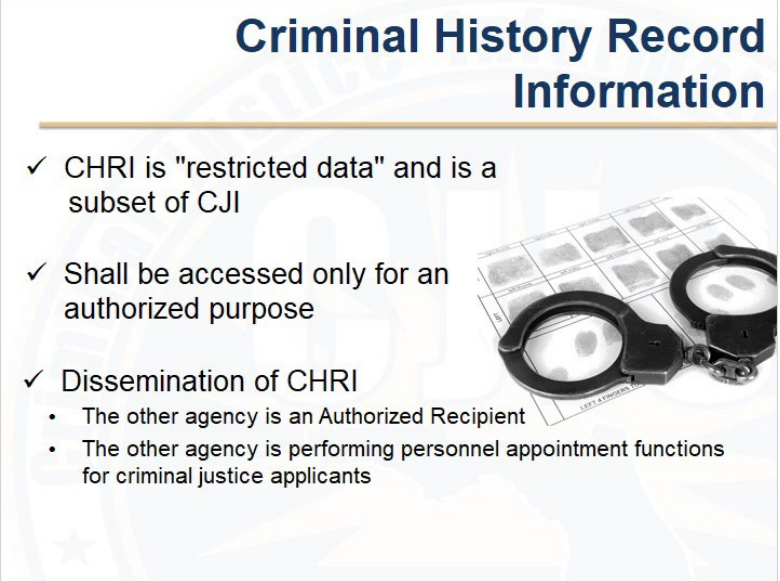

**Notes:**

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

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

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

## *1.17 Criminal History Record Information (CHRI)*

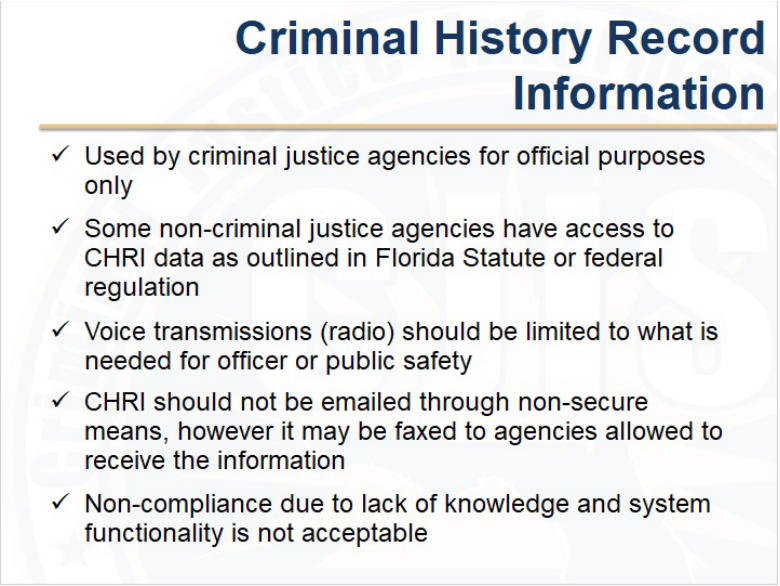



**Notes:**

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

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

## *1.18 Criminal History Record Information (CHRI)*

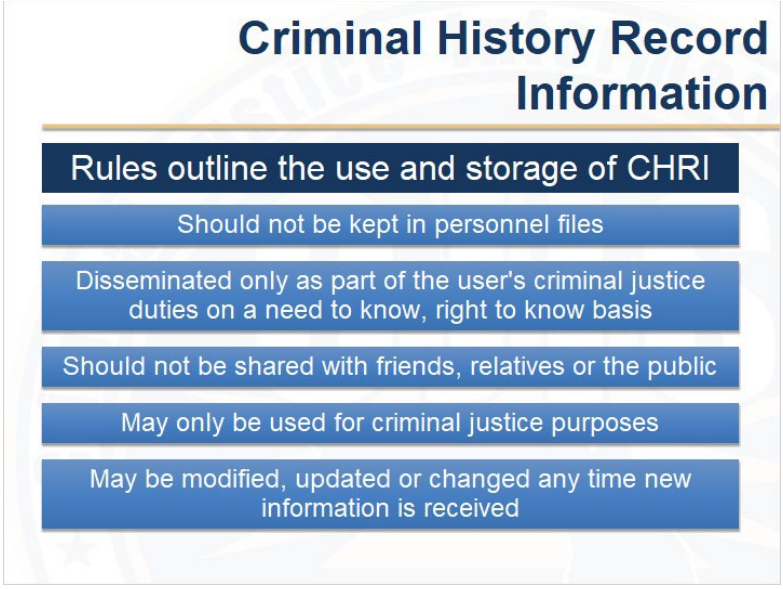



**Notes:**

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

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

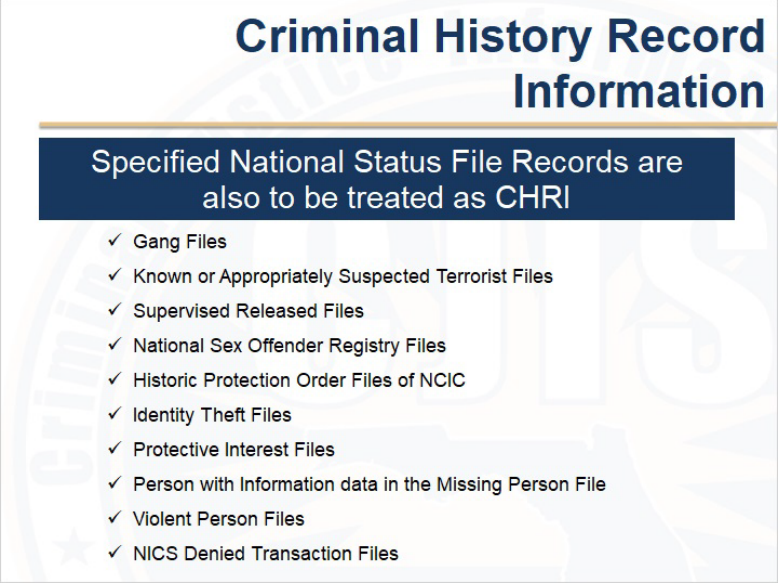
## *1.19 Criminal History Record Information (CHRI)*




**Notes:**

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

## *1.20 Criminal History Record Information (CHRI)*




**Notes:**

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

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

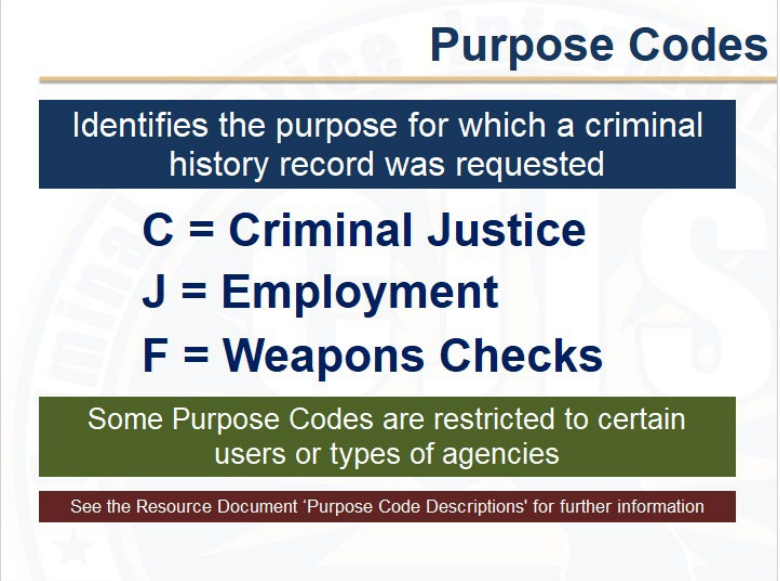
## *1.21 Alert Types*


**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.

## *1.22 Purpose Codes*

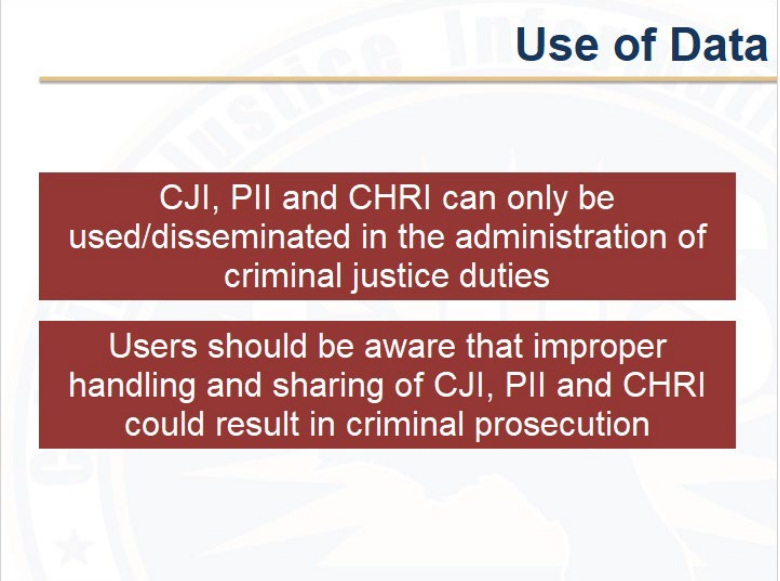



**Notes:**

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.

### *1.23 Use of Data*




**Notes:**

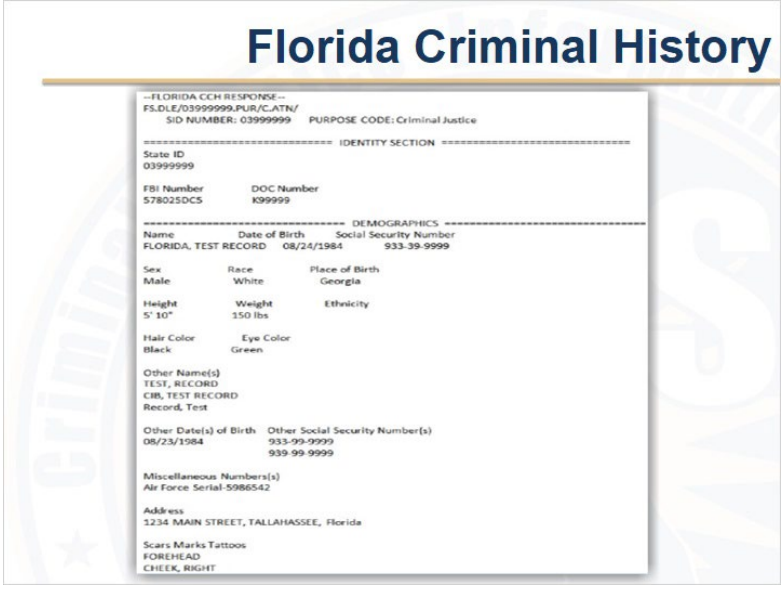
The CJI, PII and CHRI can only be used and/or disseminated in the administration of criminal justice duties. Users should be aware that the improper handling and sharing of CJI, PII and/or CHRI could result in criminal prosecution, civil fines, and termination of employment.

### *1.24 How a Florida Criminal History is Created*

**Notes:**

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

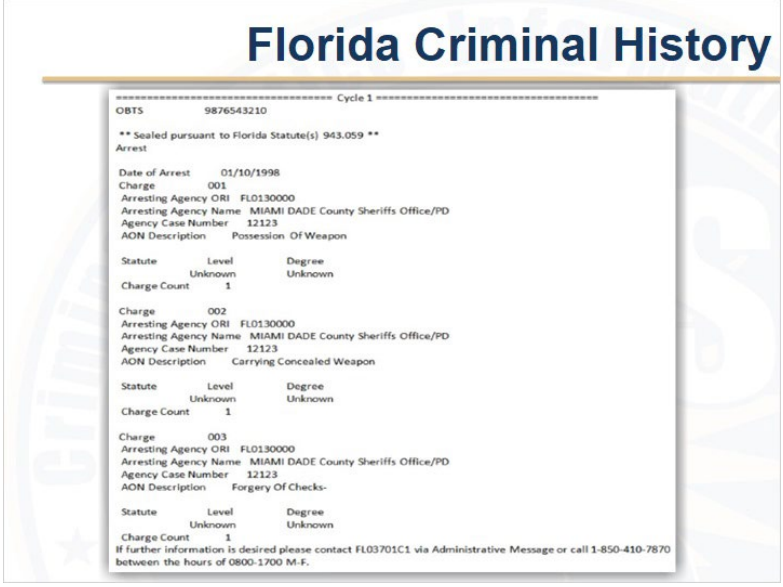
## *1.25 Florida Criminal History*




**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.

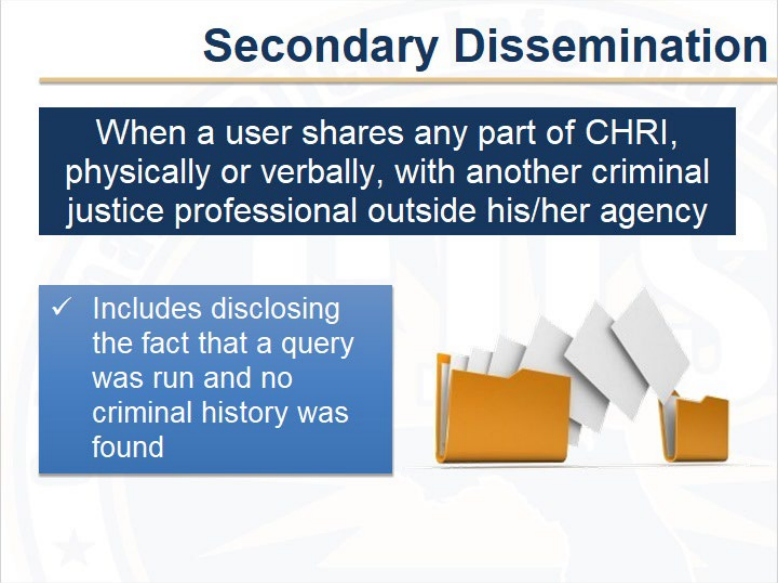
## *1.26 Florida Criminal History*




**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.

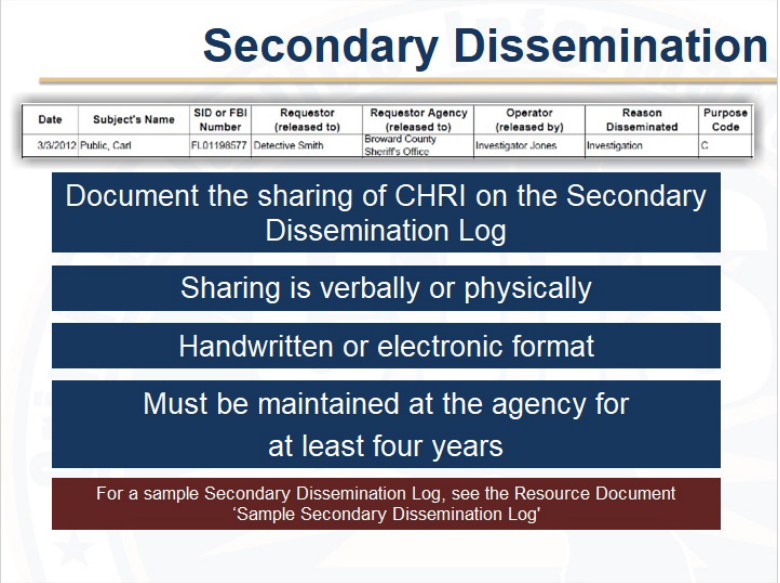
## *1.27 Secondary Dissemination*




**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 their agency. Confirming or denying the existence of Criminal History Record Information is considered Secondary Dissemination and should be documented on the Secondary Dissemination Log.

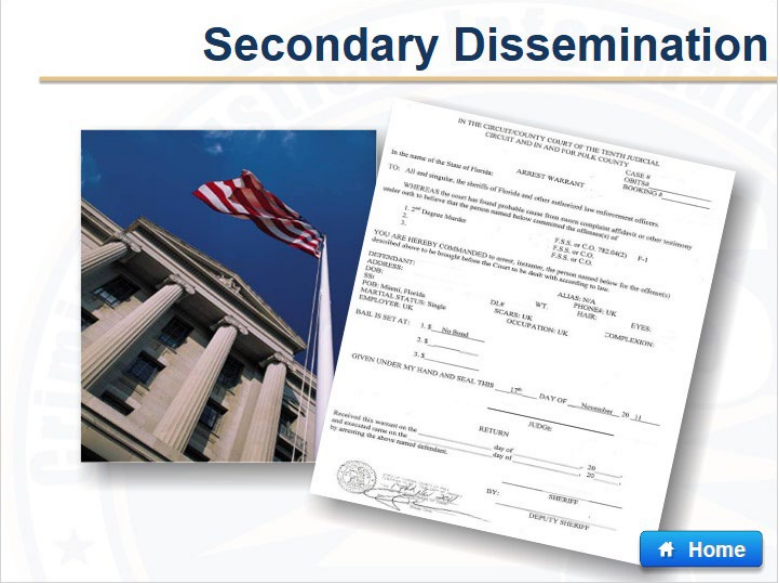
## *1.28 Secondary Dissemination Log*




**Notes:**

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

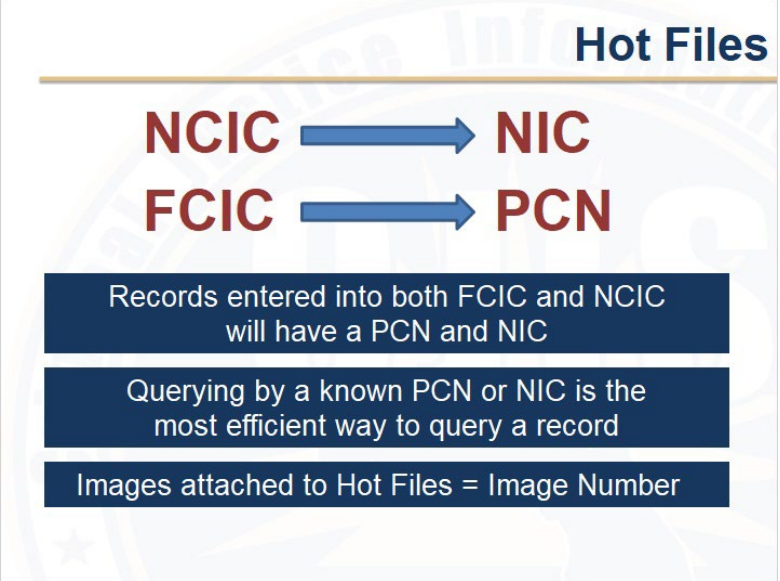
## *1.29 Secondary Dissemination*




**Notes:**

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

## *1.30 Hot Files*

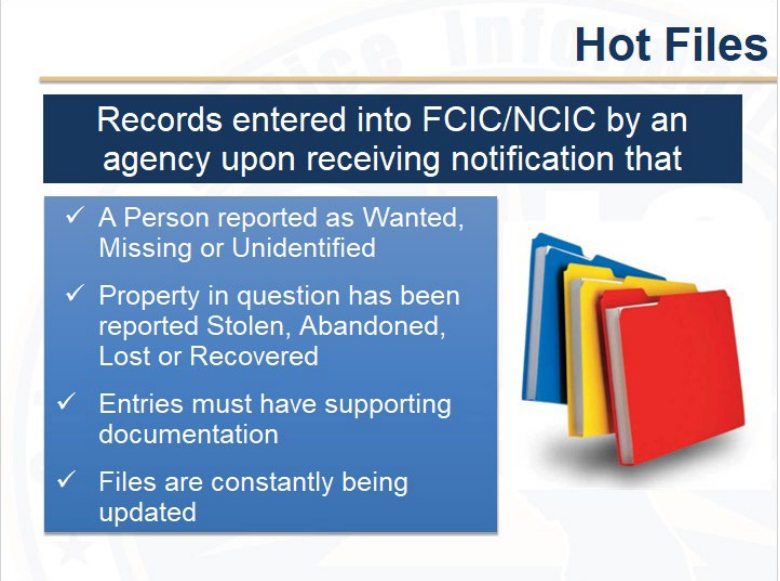



**Notes:**

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

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

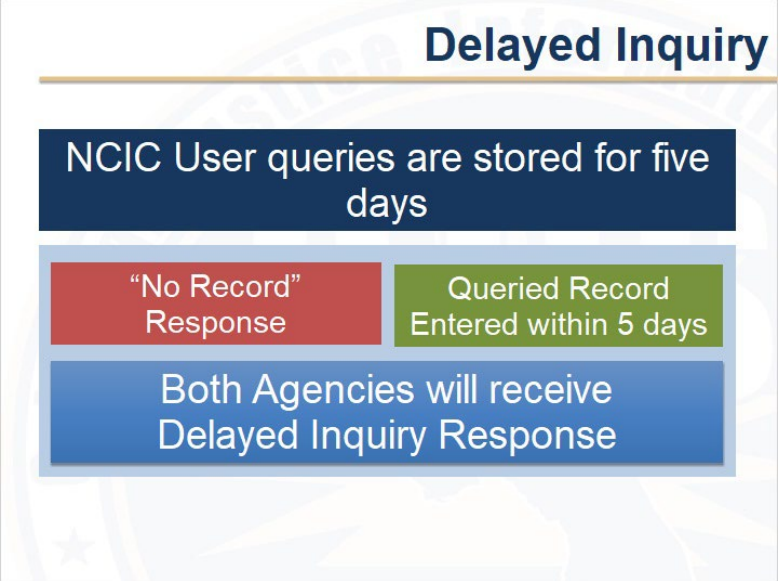
## *1.31 Hot Files*




**Notes:**

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

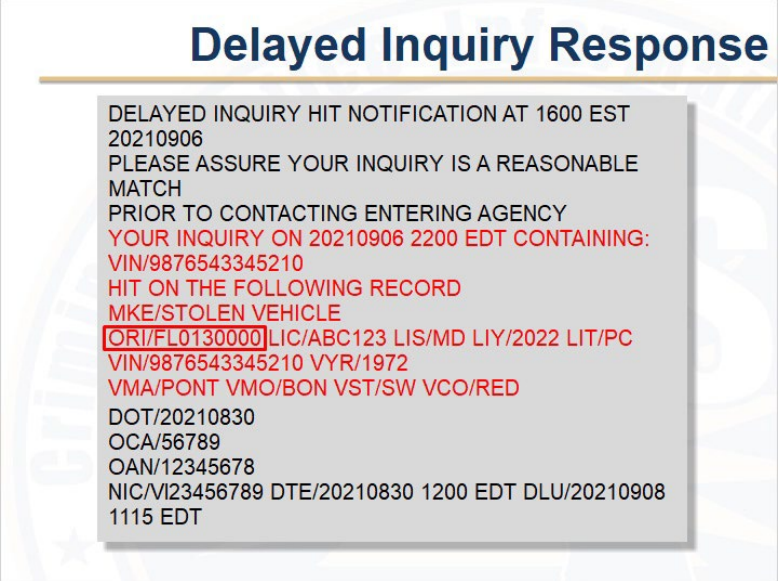
### *1.32 Delayed Inquiry*




**Notes:**

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

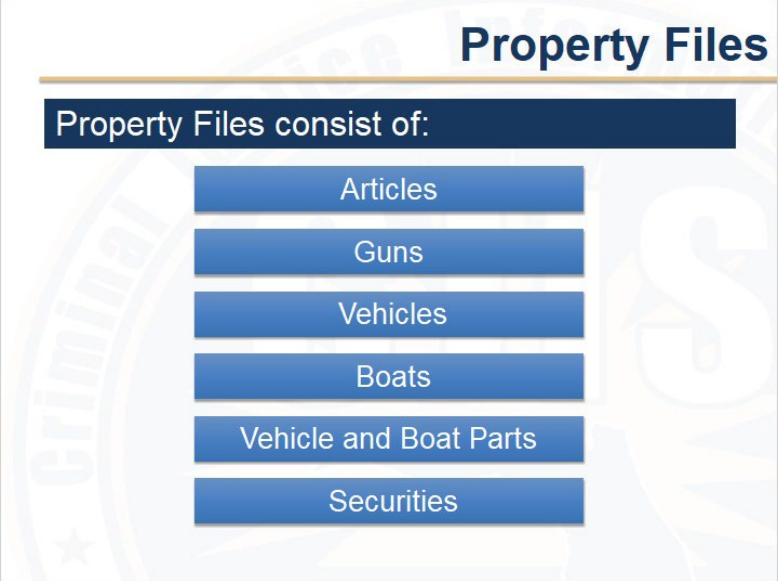
## *1.33 Delayed Inquiry Response*




**Notes:**

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

### *1.34 Property Files Introduction*




**Notes:**

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

## *1.35 Property Files*


**Notes:**

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

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

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

## *1.36 Property Files*

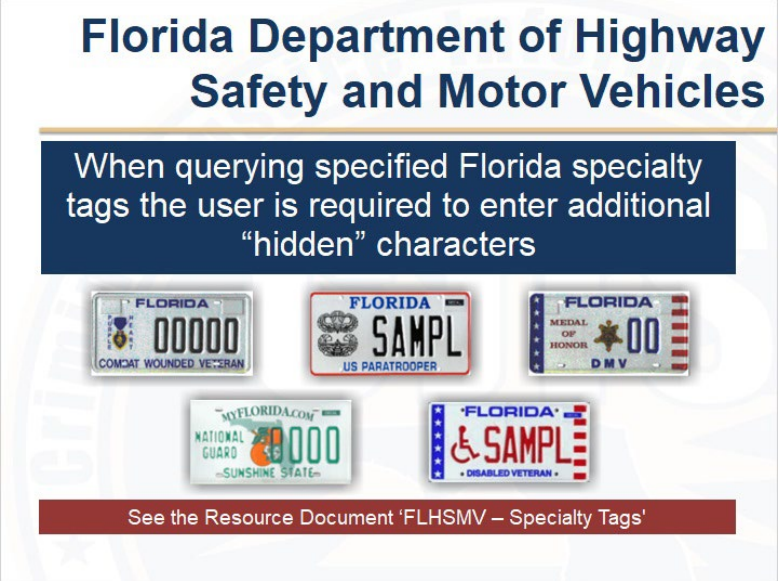

**Notes:**

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

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

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

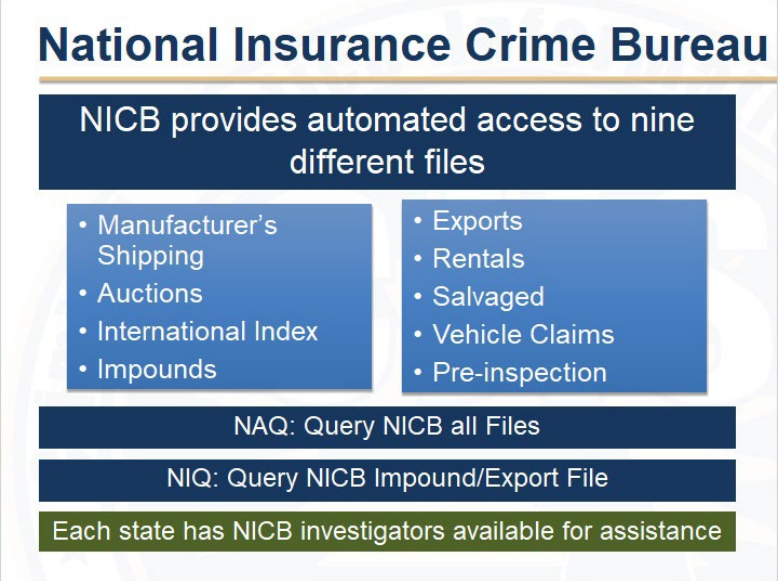
## *1.37 DHSMV*




**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 "FLHSMV – Specialty Tags" for further information on how to query these "hidden" character tags. This document can be printed for future reference.

## *1.38 NICB*




**Notes:**

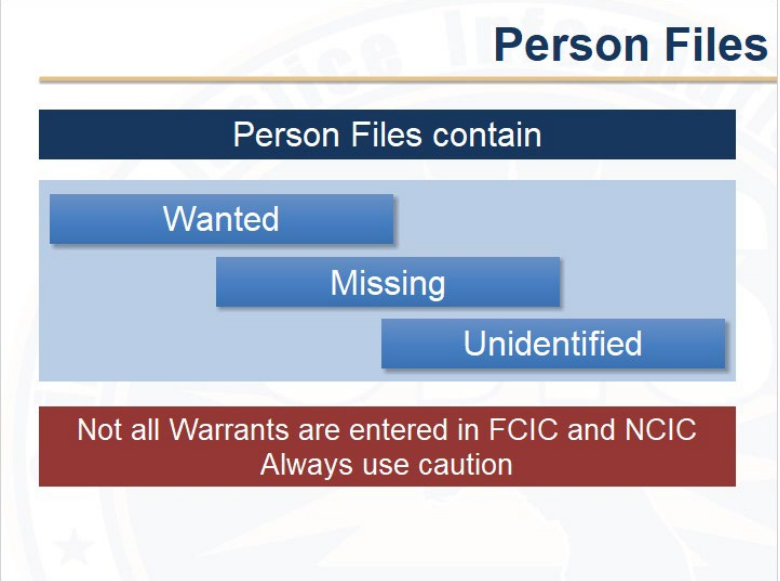
The National Insurance Crime Bureau (NICB) provides automated access to nine different files:

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

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

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

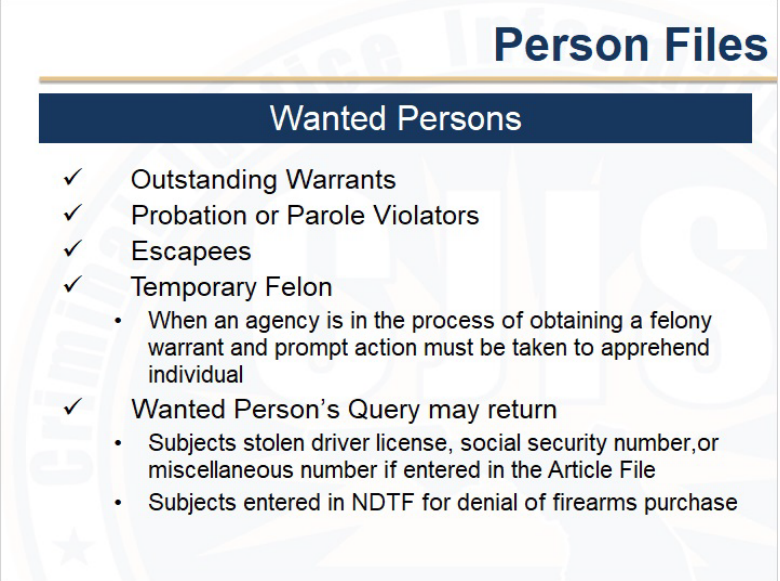
### *1.39 Person Files*




**Notes:**

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

## *1.40 Person Files*




**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.

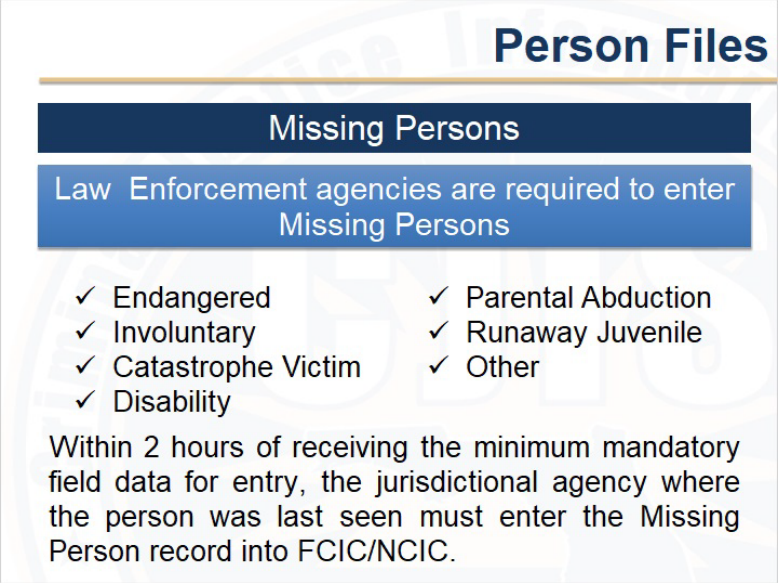
Temporary Felon records are also contained within the Person Files. A Temporary Felon record contains information on a person an agency is in the process of acquiring a felony warrant on, and determines the subject may flee; therefore, prompt action must be taken to apprehend the individual. Temporary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

### *1.41 Person Files*



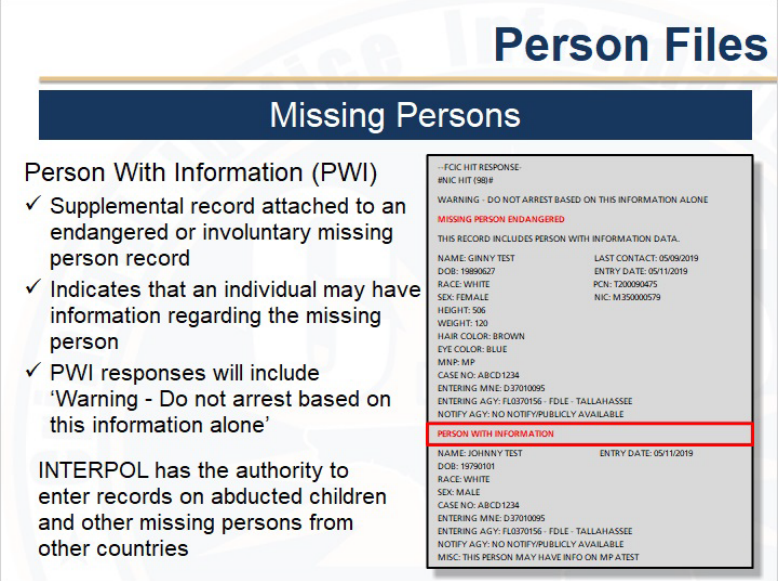

**Notes:**

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.

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.

## *1.42 Person Files*

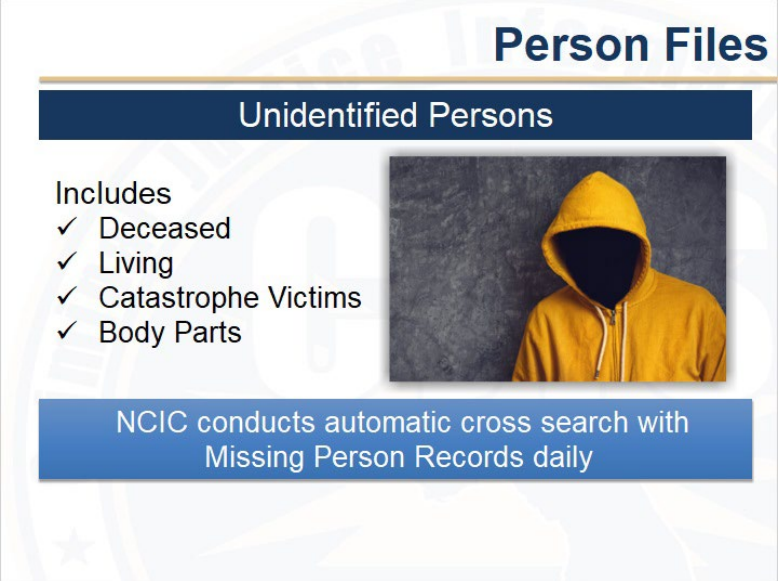



**Notes:**

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.

## *1.43 Person Files*

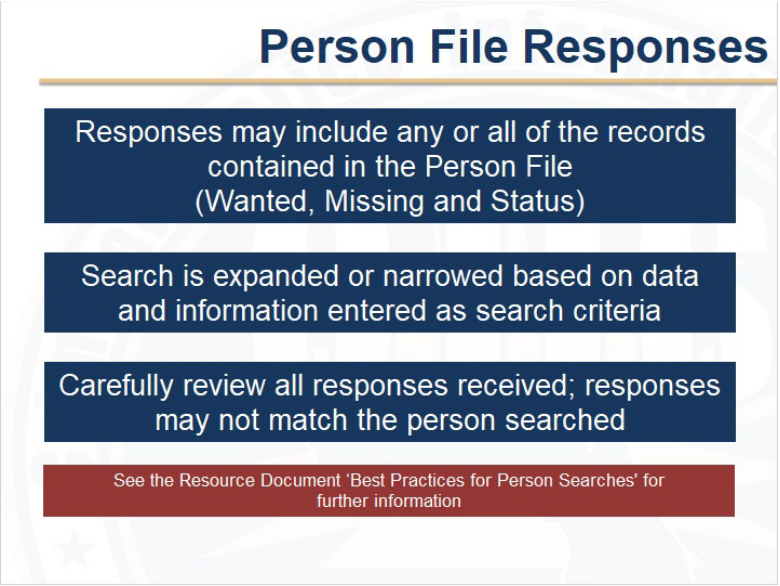



**Notes:**

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.

## *1.44 Person Files*



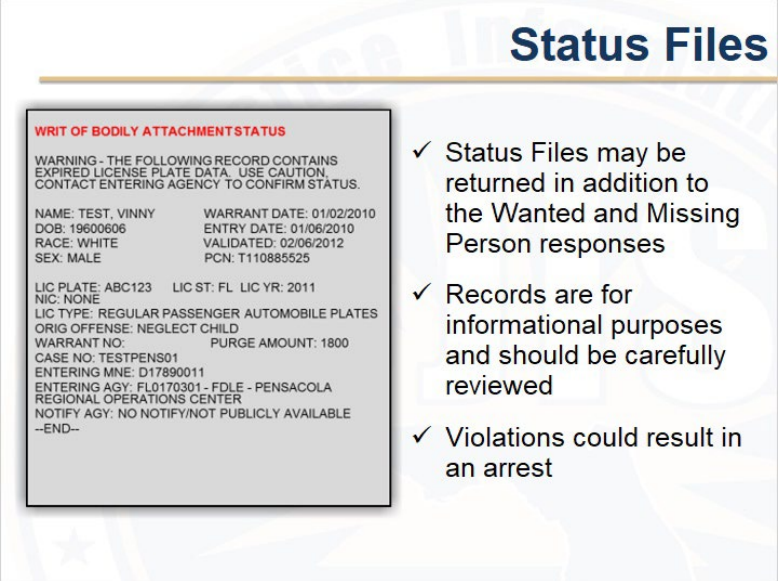

**Notes:**

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.

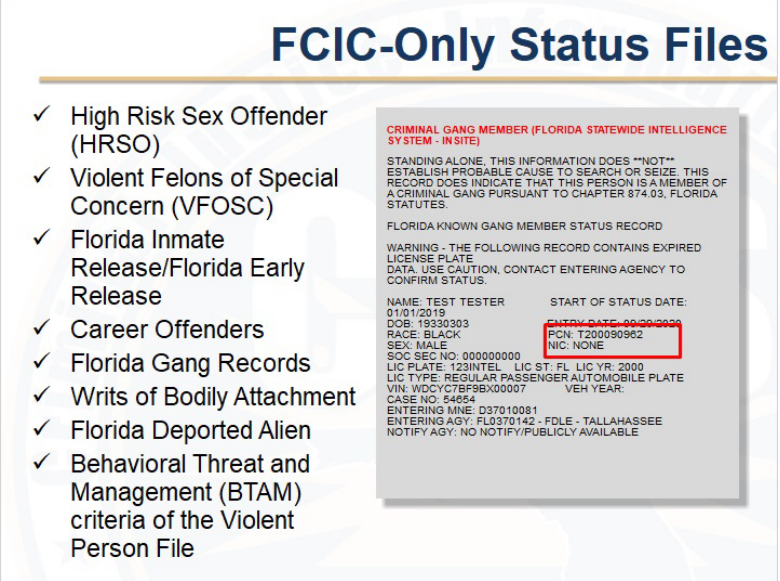
## *1.45 Status Files*




**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.

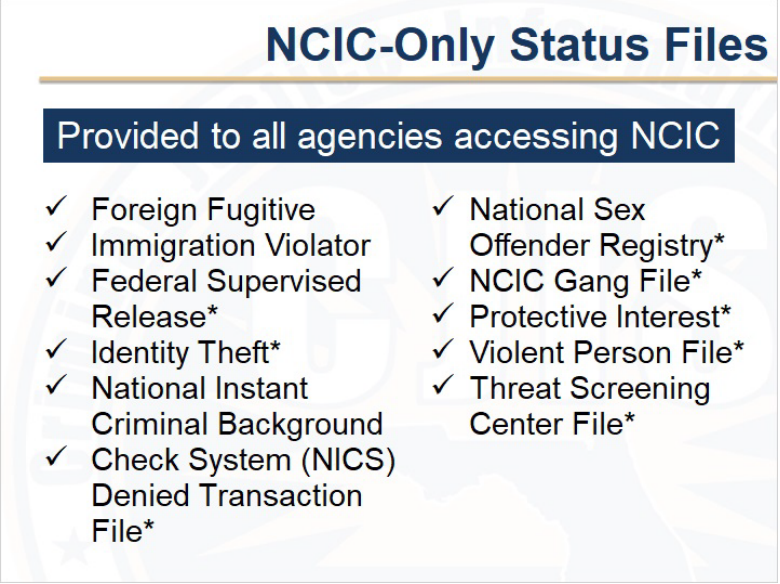
## *1.46 FCIC-Only Status Files*




**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.

### *1.47 NCIC-Only Status Files*

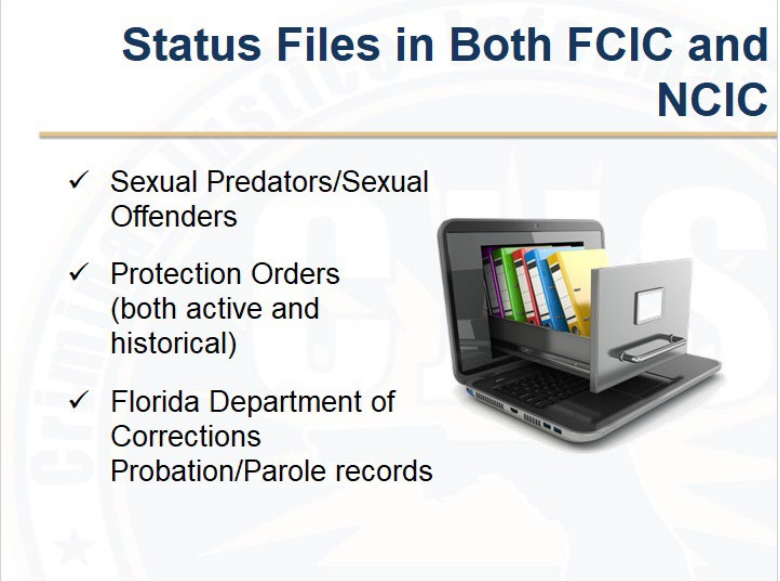



**Notes:**

NCIC-Only Status Files are provided to all agencies accessing NCIC. These files include Foreign Fugitive, Immigration Violator, Federal Supervised Release, Identity Theft, National Instant Criminal Background Check System (NICS) Denied Transaction 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.

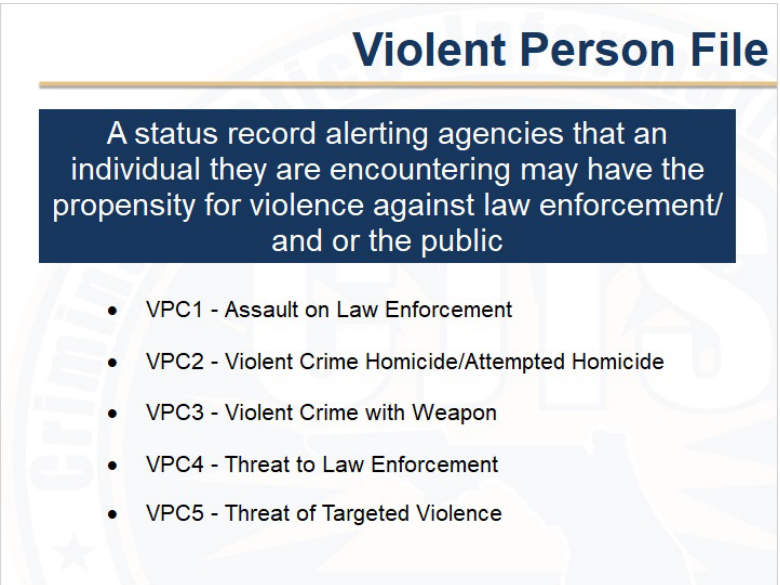
### *1.48 Status Files in both FCIC and NCIC*




**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.

### *1.49 Violent Person File*



**Notes:**

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

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

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

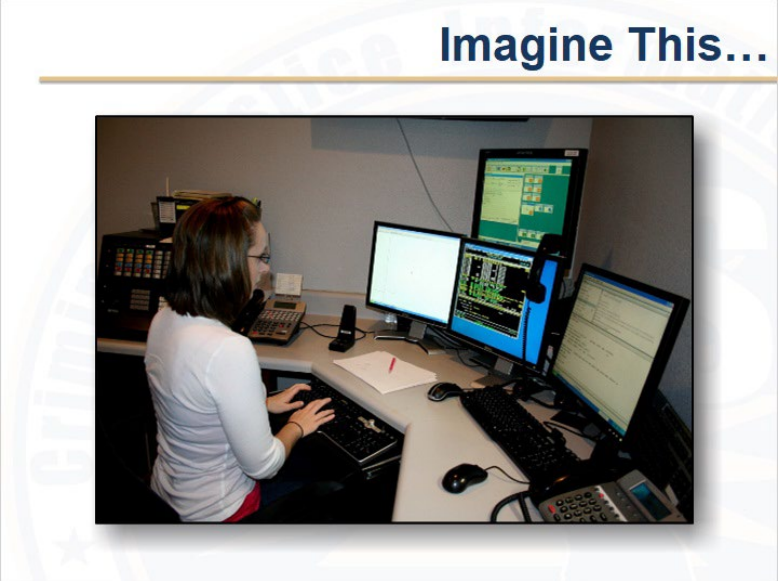
VPC 2: Violent Crime Homicide/Attempted Homicide: Offender has been convicted of a violent offense against a person to include homicide and attempted homicide.

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

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

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

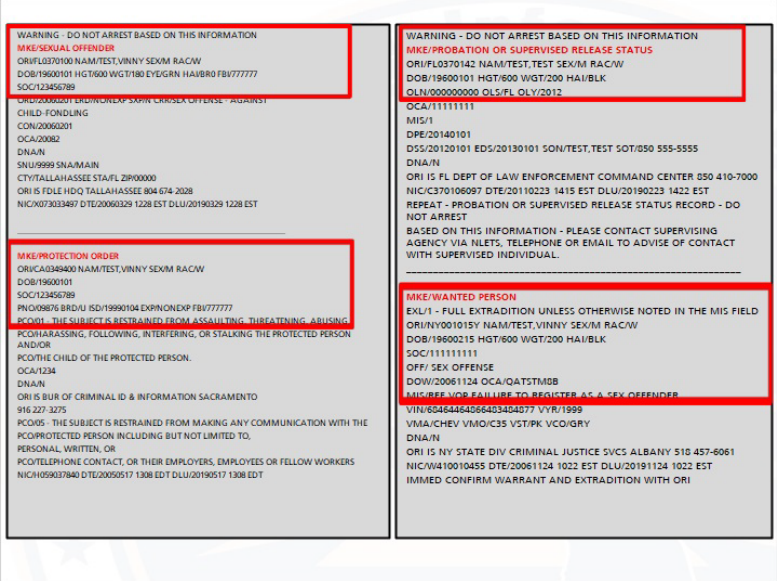
### *1.50 Imagine this…*




**Notes:**

Imagine this, you are a new dispatcher at a local police department and received 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 received 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 for assistance.

## *1.51 Imagine this scenario continued…*




**Notes:**

“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.”

“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”.

### *1.52 FCIC Agency Coordinator*


**Notes:**

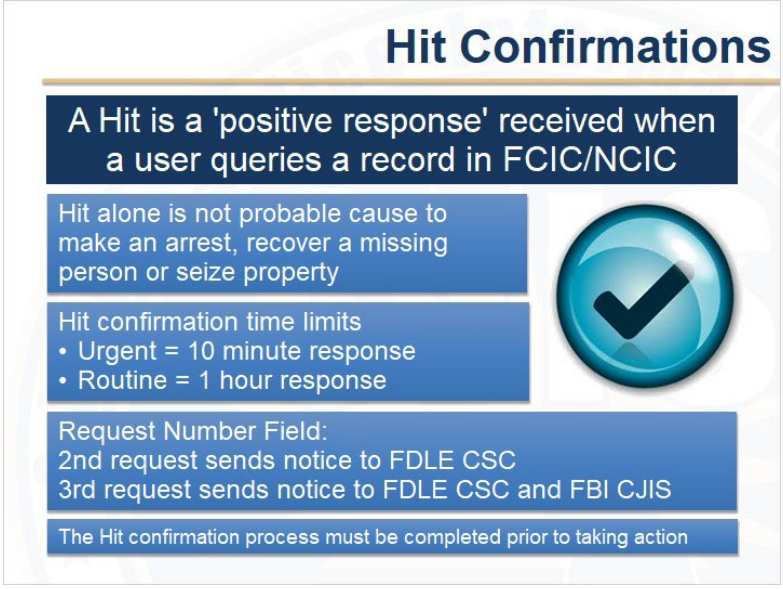
The FCIC Agency Coordinator, or FAC, serves as the agency's point of contact, both internally and externally, in matters regarding FCIC/NCIC. The FAC also serves as the liaison between the local agency and FDLE in CJIS matters. The FAC is responsible for ensuring that their agency is in compliance with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

### *1.53 FCIC Agency Coordinator*

**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 or by email at FDLECustomerSupport@fdle.state.fl.us. Select the home button to return to the main screen.

## *1.54 Hit Confirmations*




**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.

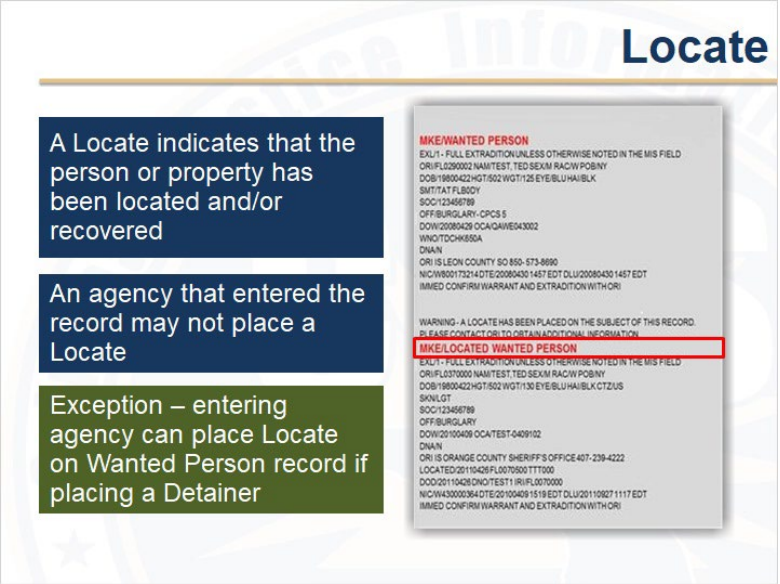
Hit Confirmation time limits are set according to the level of priority assigned by the requesting agency. Urgent hit confirmation requests require a ten-minute response, while Routine hit confirmation requests must be responded to within one hour.

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*

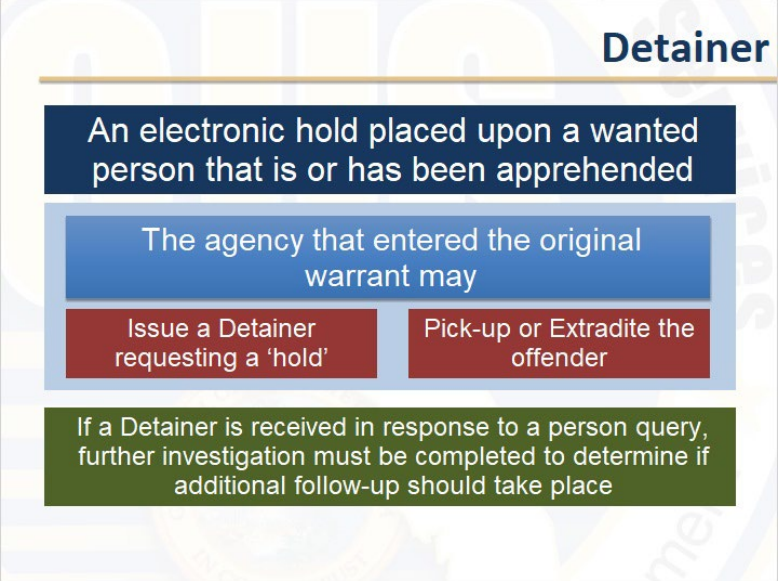



**Notes:**

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 own 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.

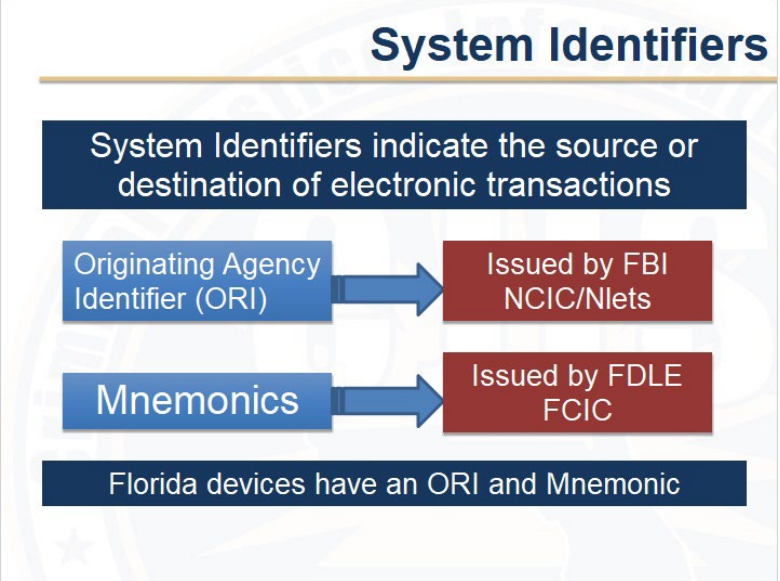
## *1.56 Detainer*




**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 System Identifiers*

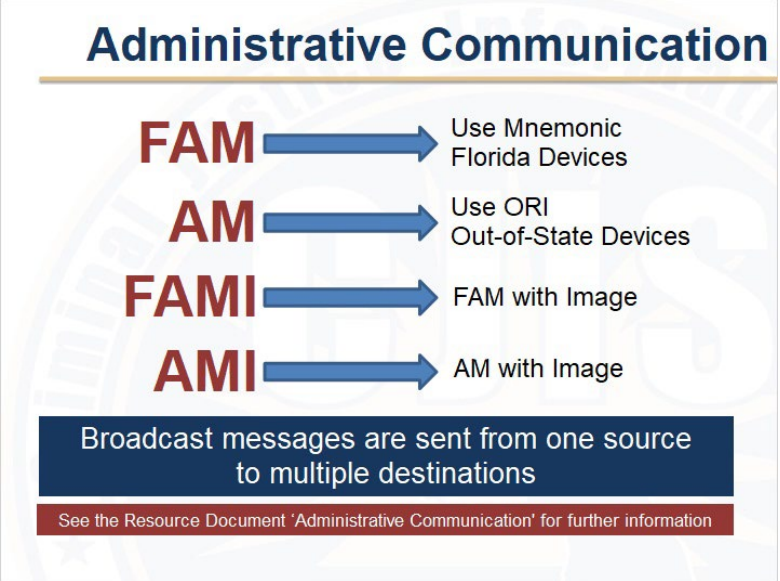



**Notes:**

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

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

## *1.58 Administrative Communication*




**Notes:**

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

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

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

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

## *1.59 Guidelines for Communication*


**Notes:**

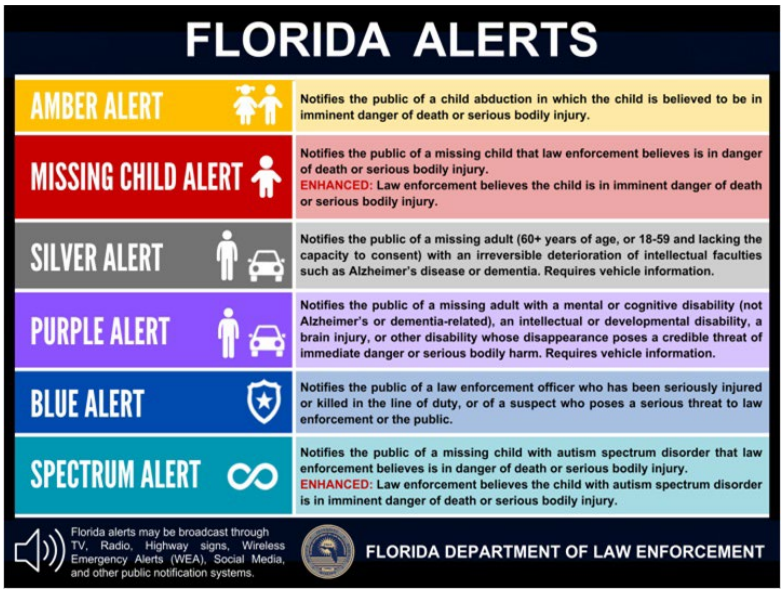
Users must follow basic guidelines when sending an administrative communication. These guidelines include using plain English, not using 10 codes or signal codes, not sending non-law enforcement related information such as personal messages, holiday greetings, job or retirement notices, and press releases.

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.

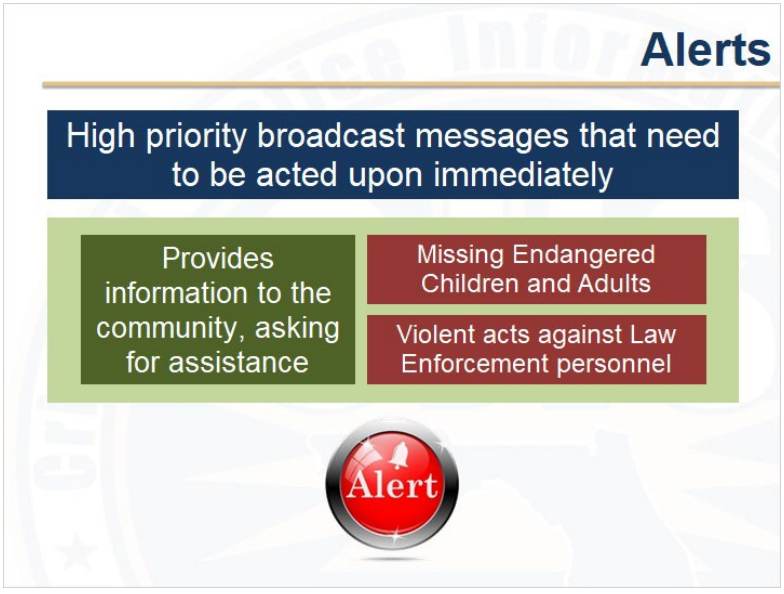
## *1.60 Untitled Slide*




**Notes:**

In the next few slides we will discuss each of the Florida Alert types.

## *1.61 Alerts Introduction*




**Notes:**

There are certain special types of messages or Alerts that users should pay particular attention to. These are high priority notifications that need to be acted upon immediately.

---

These alerts provide information to the community asking for assistance in the recovery of missing, endangered children or adults. Additionally, they provide information on violent acts against law enforcement personnel.

### *1.62 Alert Types*


**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”.

## *1.63 Alert Types*


**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.

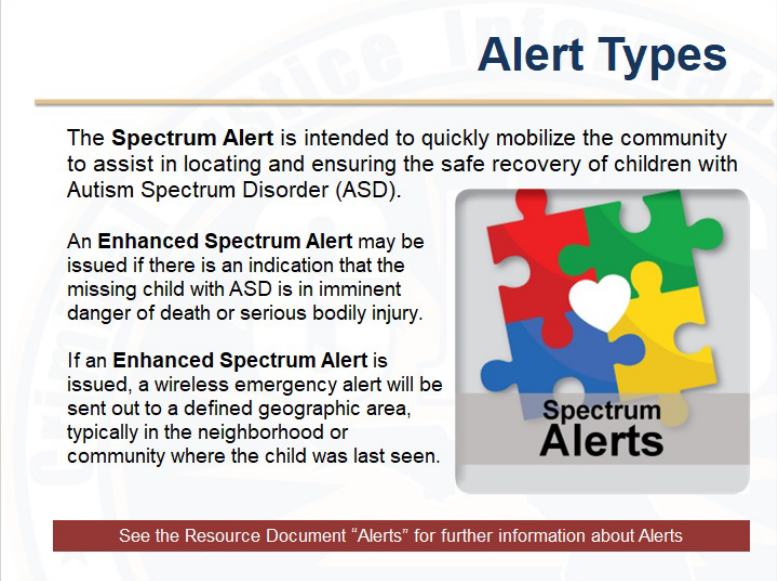
The Purple Alert must be disseminated to the geographic areas where the missing adult could reasonably be, considering his/her circumstances and physical and mental condition, the potential modes of transportation available, and the known or suspected circumstances of his/her disappearance.

## *1.64 Alert Types*


**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, Purple, and Blue Alerts.

## *1.65 Alert Types*



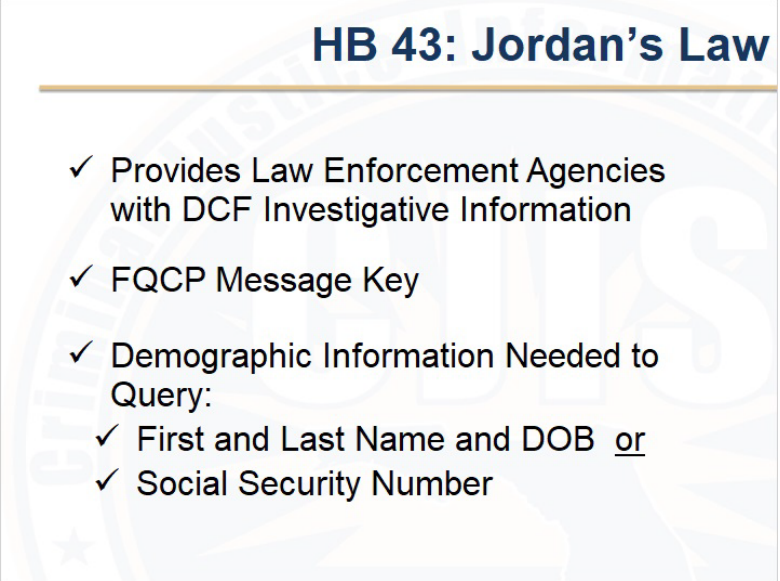

**Notes:**

**The Spectrum Alert is intended to quickly mobilize the community to assist in locating and ensuring the safe recovery of children with autism spectrum disorder**.

**An Enhanced Spectrum Alert may be issued if there is an indication that the missing child with ASD is in imminent danger of death or serious bodily injury. If an Enhanced Spectrum Alert id issues, a wireless emergency alert will be sent out to a defined geographic area, typically in the neighborhood or community where the child was last seen.**

**See the Resource Document "Alerts" for further information about Alerts.**

## *1.66 Jordan's Law*

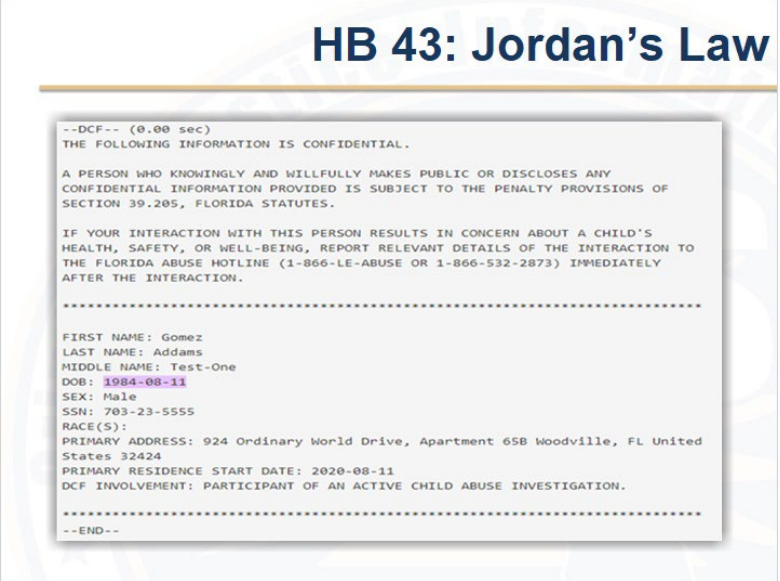



**Notes:**

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.

## *1.67 Jordan's Law*




**Notes:**

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

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

If a law enforcement officer is concerned about a child's health and safety, they shall reach out to the Florida Abuse Hotline number 1-800-962-2873 which is also provided within the caveat of the response.

## *1.68 Identity Theft*

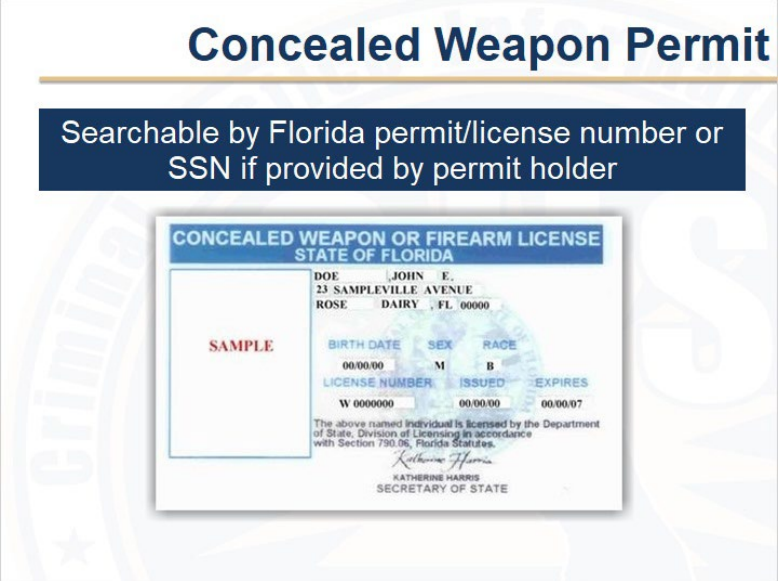

**Notes:**

When a person becomes aware that their 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 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.

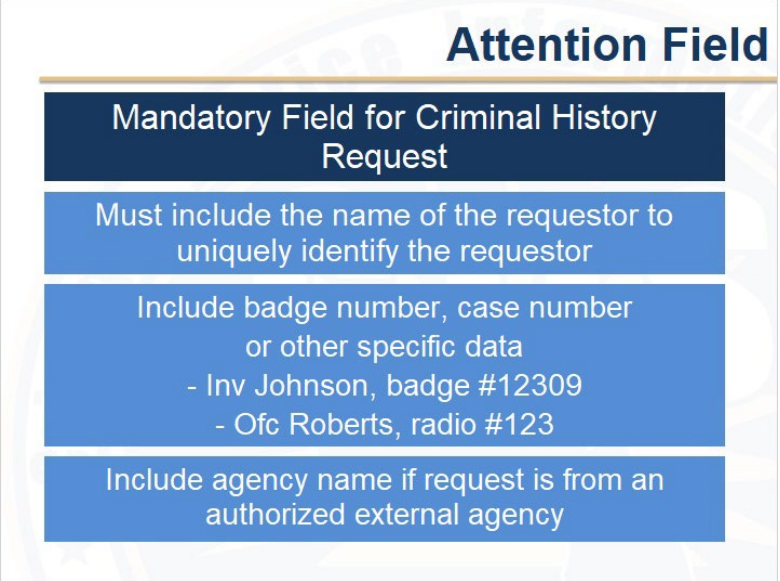
## *1.69 Concealed Weapon Permit*




**Notes:**

Concealed Weapon Licenses 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. A 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.

## *1.70 Attention Field*




**Notes:**

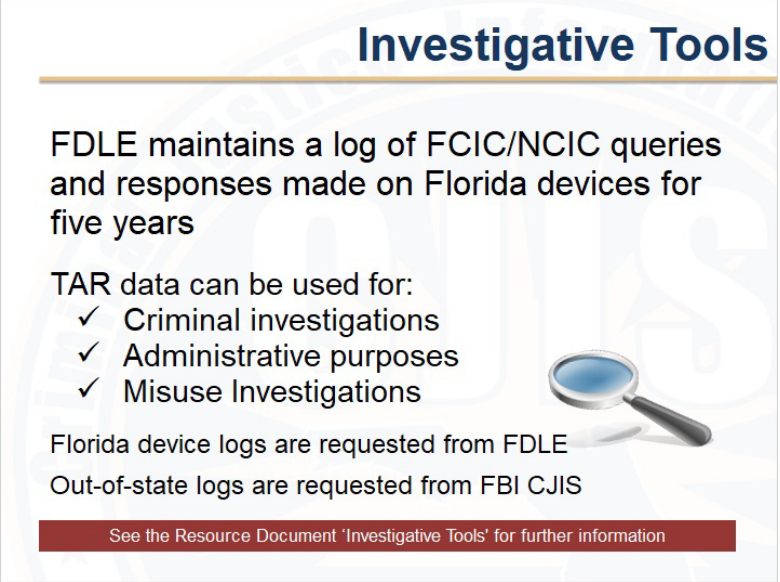
The Attention Field is mandatory and must contain the name of the person requesting the CHRI, to uniquely identify the requestor of the CHRI. In addition to the requestor's name, a badge number, case number or other specific data should be included to assist in identifying them and the purpose of the 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.

### *1.71 Concealed Weapon Permit*


**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.

### *1.72 Investigative Tools*

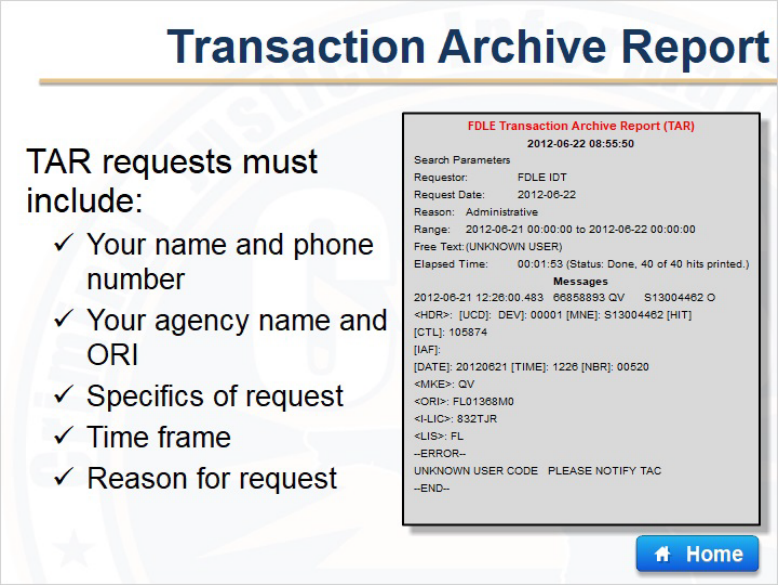



**Notes:**

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 for 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.

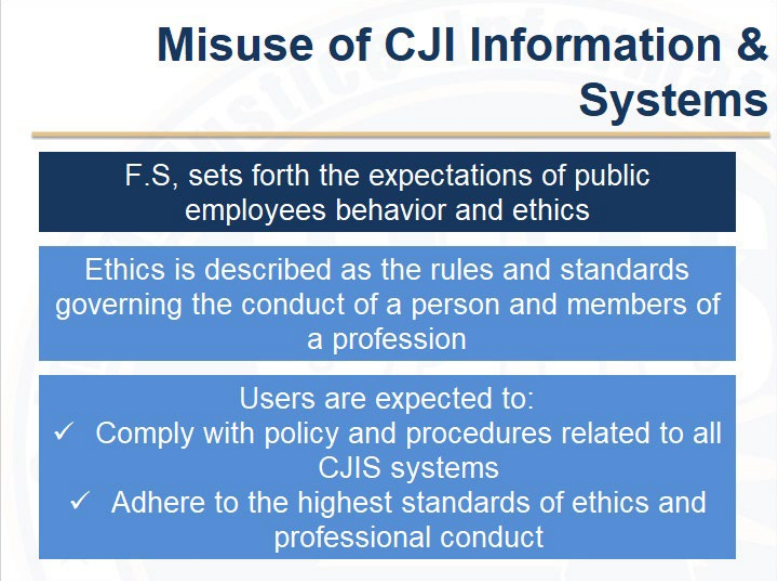
## *1.73 Transaction Archive Report (TAR)*




**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. Select the home button to return to the main screen.

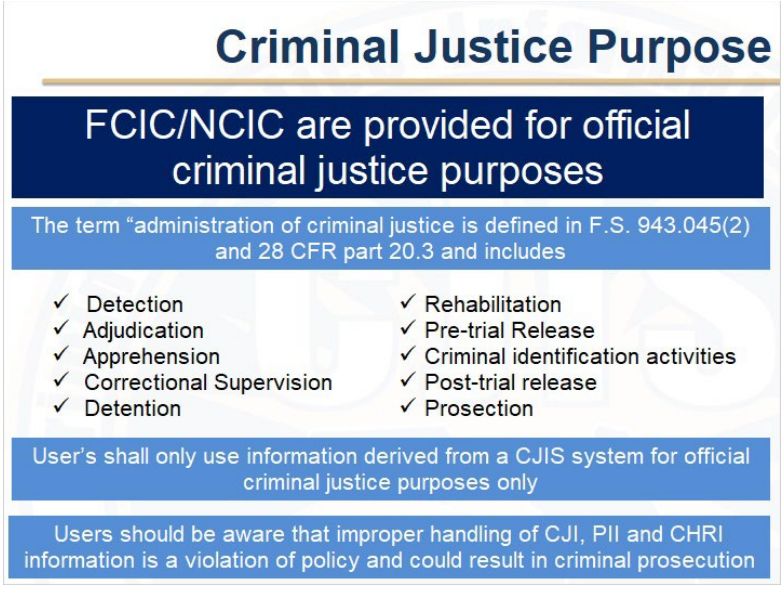
## *1.74 Misuse of Criminal Justice Information (CJI)*




**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.

## *1.75 Common Types of Misuse*

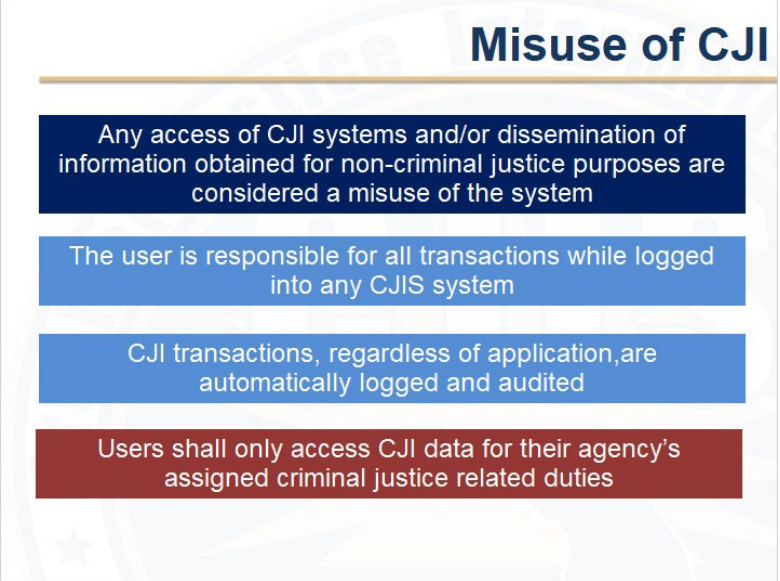



**Notes:**

FCIC and NCIC is 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, PI I, 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.

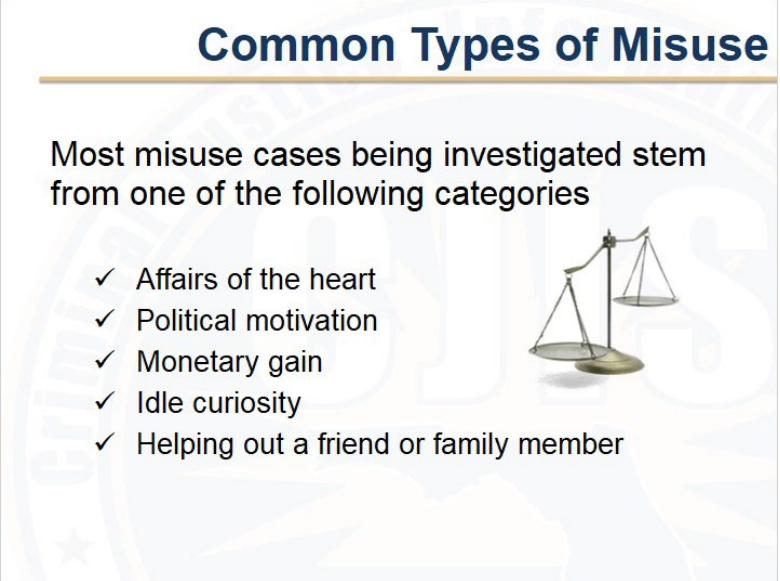
## *1.76 Common Types of Misuse*




**Notes:**

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

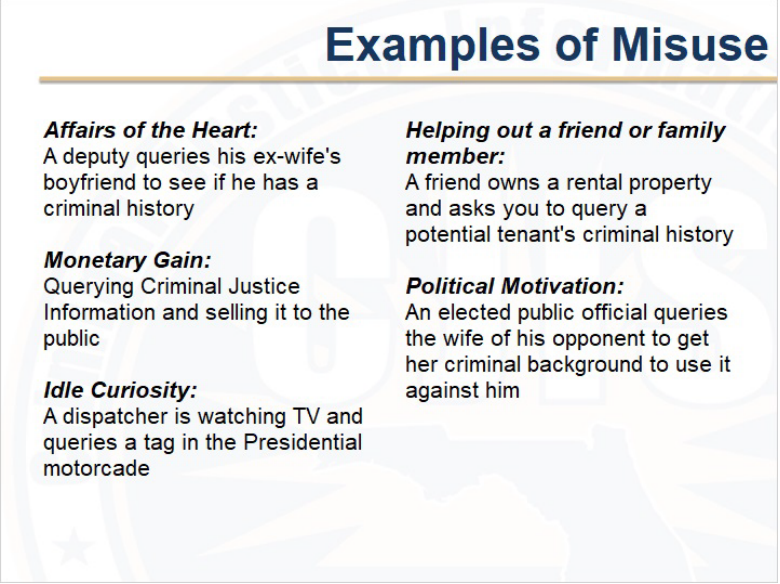
## *1.77 Common Types of Misuse*




**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.

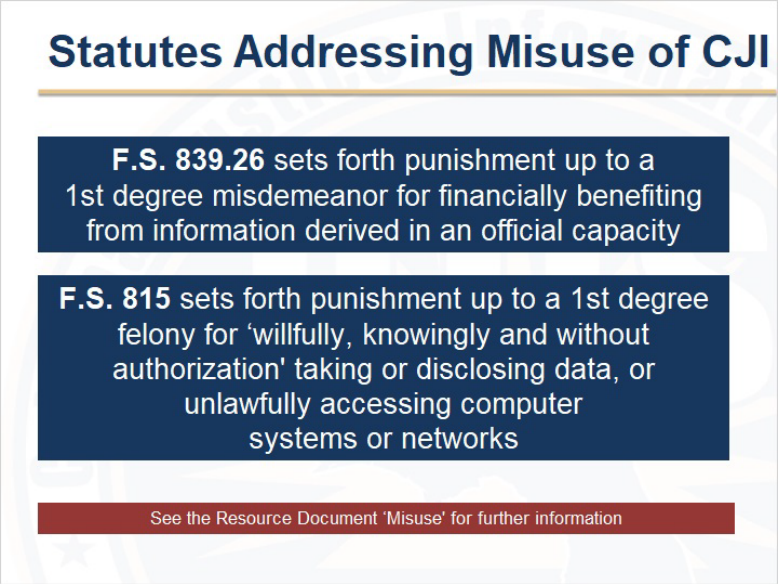
## *1.78 Examples of Misuse*




**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.

### *1.79 Statutes Addressing Misuse of CJI*




**Notes:**

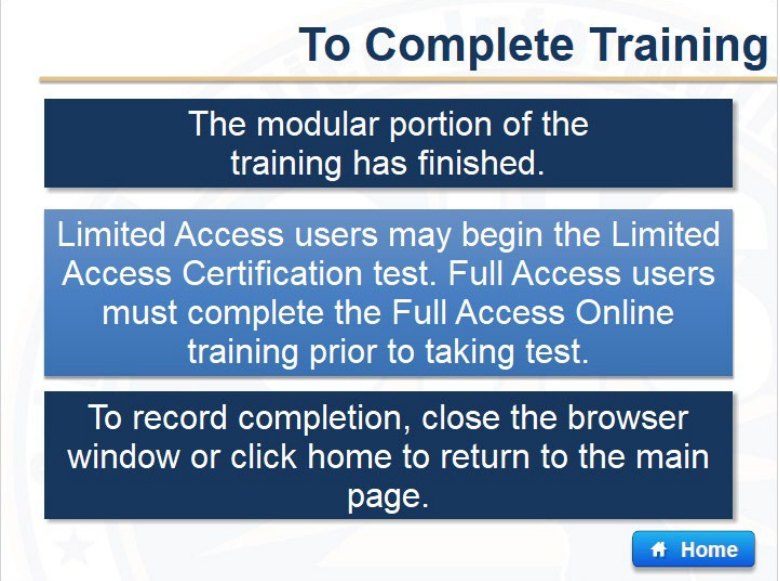
The following are Florida Statutes which address the misuse of CJI. These statutes reference both ethical and criminal violations which could be grounds for disciplinary action or termination.

**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".

### *1.80 You are Ready to Test*




**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.

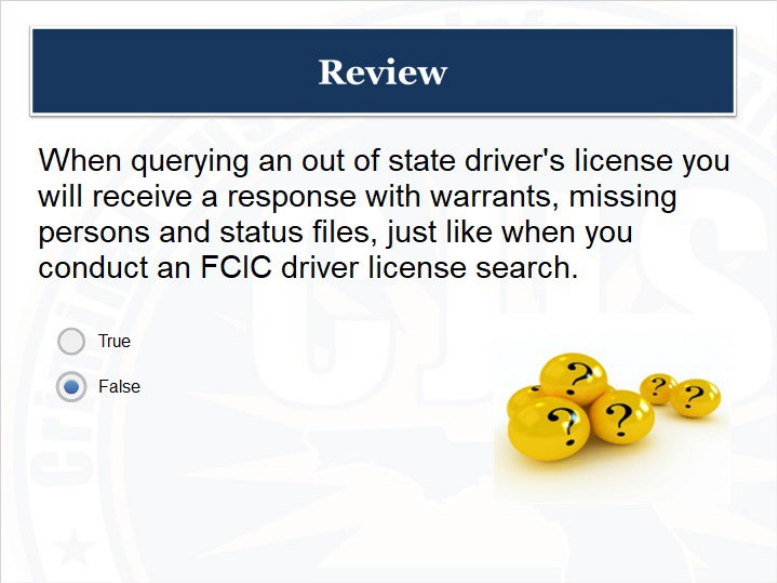
The Security and Privacy General Role training must be completed in **nexTEST** prior to the Limited Access Certification test. The test will not be available if the General Role training is not completed prior to testing.

To record completion of this training, please close the browser window.

## 1. Question Bank 1

### *Q1.1 Review Slide 1*

*(True/False, 10 points, 2 attempts permitted)*




| Correct | Choice |
|---|---|
| | True |
| X | False |

**Feedback when correct:**

Correct! No automatic person search occurs with an out of state DL query.

**Feedback when incorrect:**

You did not select the correct response. Remember that an Nlets query may not provide automatic persons searches.

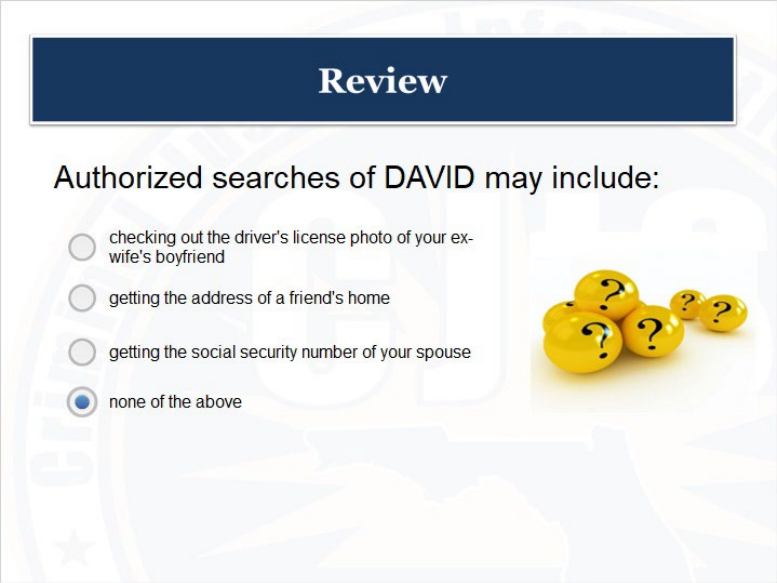
**Notes:**

Let's review what you have learned.

## *Q1.2 Review Slide 2*

*(Multiple Choice, 10 points, unlimited attempts permitted)*

---




| Correct | Choice |
|---|---|
| | checking out the driver's license photo of your ex-wife's boyfriend |
| | getting the address of a friend's home |
| | getting the social security number of your spouse |
| X | none of the above |

**Feedback when correct:**

That's right!  You selected the correct response. None of the  examples are authorized searches of DAVID.

**Feedback when incorrect:**

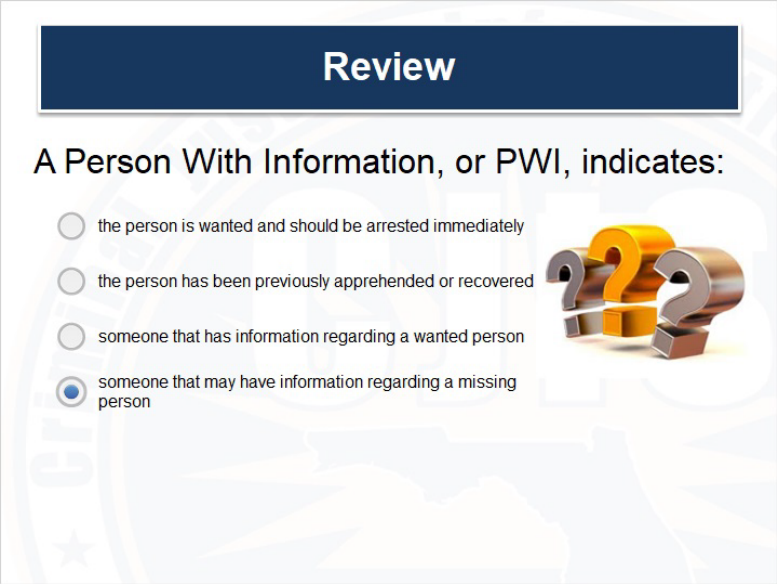
You did not select the correct response. Please carefully consider appropriate uses of DAVID.

**Notes:**

Let's review what you have learned.

## *Q1.3 Review Slide 3*

*(Multiple Choice, 10 points, unlimited attempts permitted)*




| Correct | Choice |
|---|---|
| | the person is wanted and should be arrested immediately |
| | the person has been previously apprehended or recovered |
| | someone that has information regarding a wanted person |
| X | someone that may have information regarding a missing person |

**Feedback when correct:**

That's right!  A PWI may provide additional information regarding a missing person.

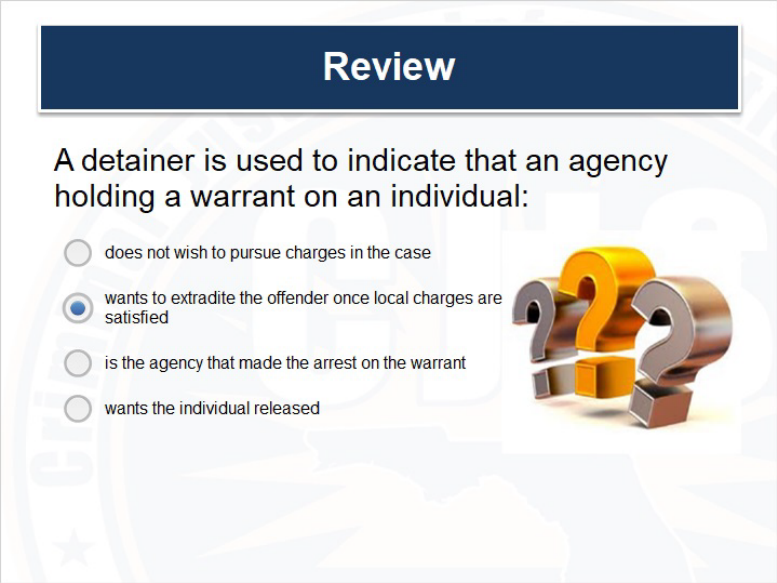
**Feedback when incorrect:**

You did not select the correct response.

## *Q1.4 Review Slide 4*

*(Multiple Choice, 10 points, unlimited attempts permitted)*

---




| Correct | Choice |
|---|---|
| | does not wish to pursue charges in the case |
| X | wants to extradite the offender once local charges are satisfied |
| | is the agency that made the arrest on the warrant |
| | wants the individual released |

**Feedback when correct:**

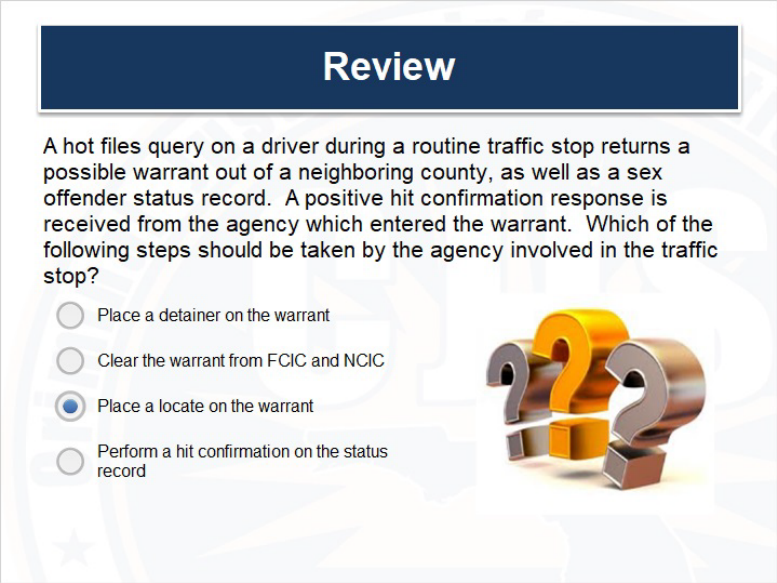
That's right!  You selected the correct response.

**Feedback when incorrect:**

You did not select the correct response.

## *Q1.5 Review Slide 5*

*(Multiple Choice, 10 points, unlimited attempts permitted)*




| Correct | Choice |
|---|---|
| | Place a detainer on the warrant |
| | Clear the warrant from FCIC and NCIC |
| X | Place a locate on the warrant |
| | Perform a hit confirmation on the status record |

**Feedback when correct:**

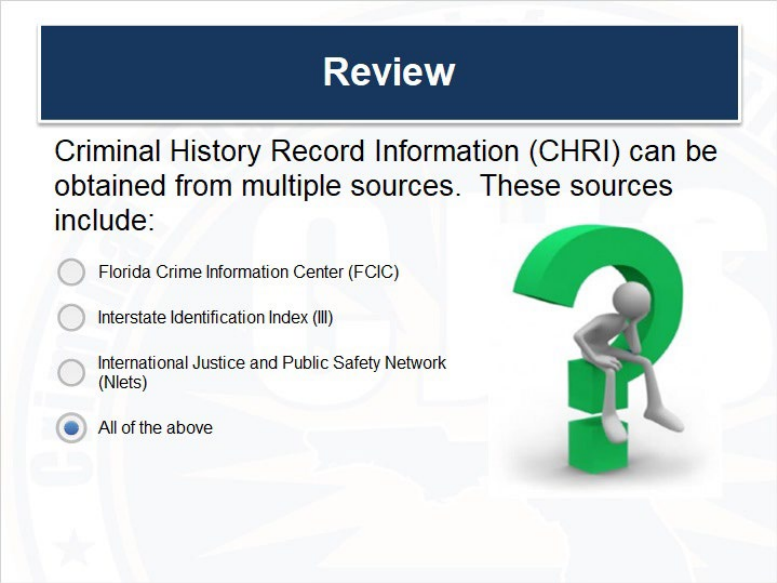
That's right! A Locate indicates the person for whom the warrant was issued has been found.

**Feedback when incorrect:**

You did not select the correct response.

## *Q1.6 Review Slide 6*

*(Multiple Choice, 10 points, unlimited attempts permitted)*




| Correct | Choice |
|---|---|
| | Florida Crime Information Center (FCIC) |
| | Interstate Identification Index (III) |
| | International Justice and Public Safety Network (Nlets) |
| X | All of the above |

**Feedback when correct:**

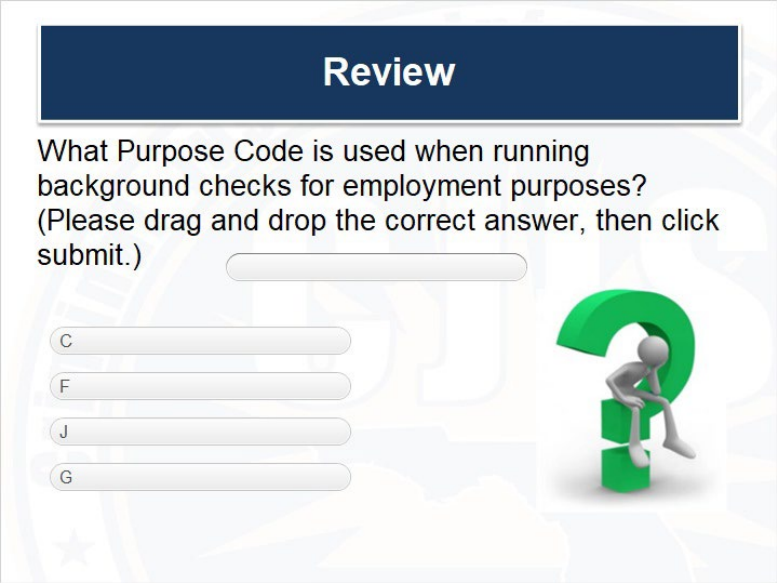
That's right! ！CHRI can be obtained from FCIC, III, and Nlets.

**Feedback when incorrect:**

You did not select the correct response.

## *Q1.7 Review Slide 7*

*(Word Bank, 10 points, unlimited attempts permitted)*




| Correct | Choice |
|---|---|
| | C |
| | F |
| X | J |
| | G |

**Feedback when correct:**

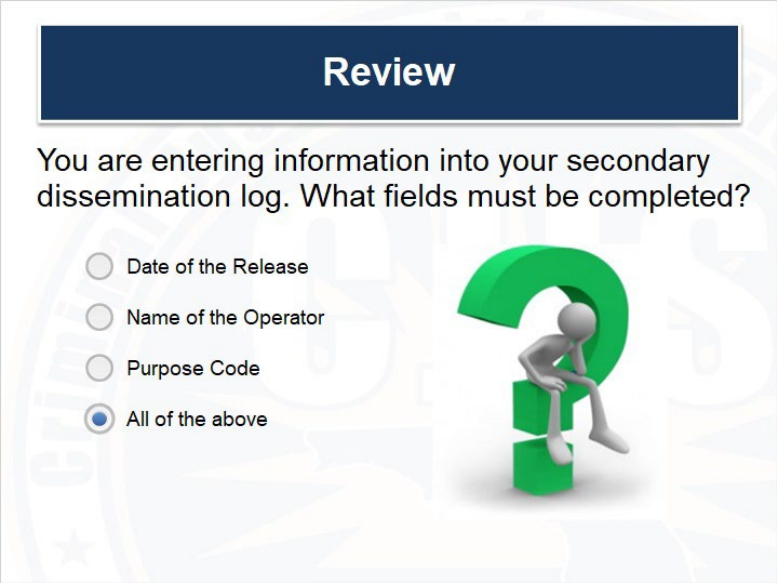
That's right!  Purpose Code J is used for Criminal Justice Employment.

**Feedback when incorrect:**

You did not select the correct response.

## *Q1.8 Review Slide 8*

*(Multiple Choice, 10 points, unlimited attempts permitted)*




| Correct | Choice |
|---|---|
| | Date of the Release |
| | Name of the Operator |
| | Purpose Code |
| X | All of the above |

**Feedback when correct:**

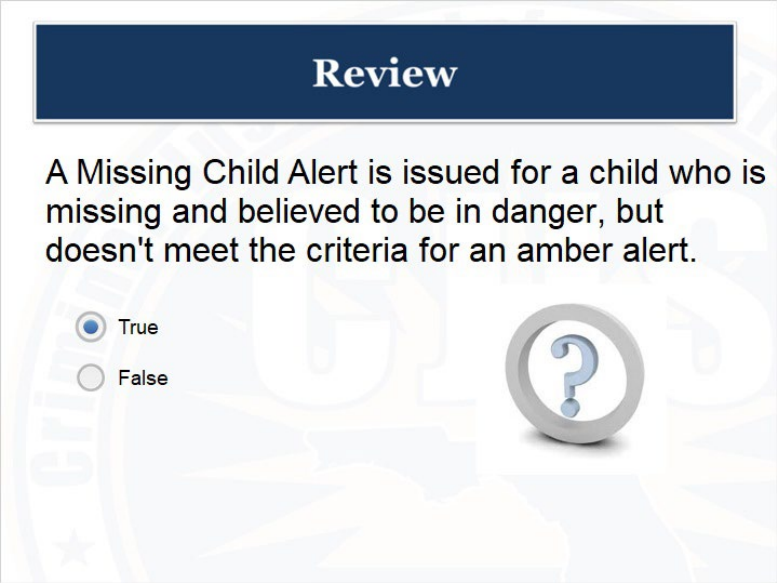
That's right!  All of these fields must entered into the secondary dissemination log.

**Feedback when incorrect:**

You did not select the correct response.

## *Q1.9 Review Slide 9*

*(True/False, 10 points, 4 attempts permitted)*




| Correct | Choice |
|---|---|
| X | True |
| | False |

**Feedback when correct:**

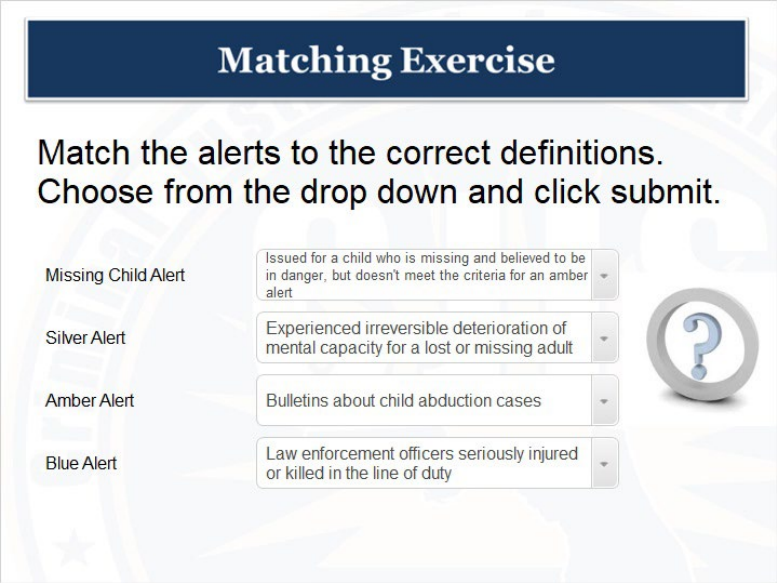
That's right!  You selected the correct response.

**Feedback when incorrect:**

You did not select the correct response.

## *Q1.10 Review Slide 10*

*(Matching Drop-down, 10 points, 4 attempts permitted)*




| Correct | Choice |
|---|---|
| Missing Child Alert | Issued for a child who is missing and believed to be in danger, but doesn't meet the criteria for an amber alert |
| Silver Alert | Experienced irreversible deterioration of mental capacity for a lost or missing adult |
| Amber Alert | Bulletins about child abduction cases |
| Blue Alert | Law enforcement officers seriously injured or killed in the line of duty |

**Feedback when correct:**

That's right!  You selected the correct response.

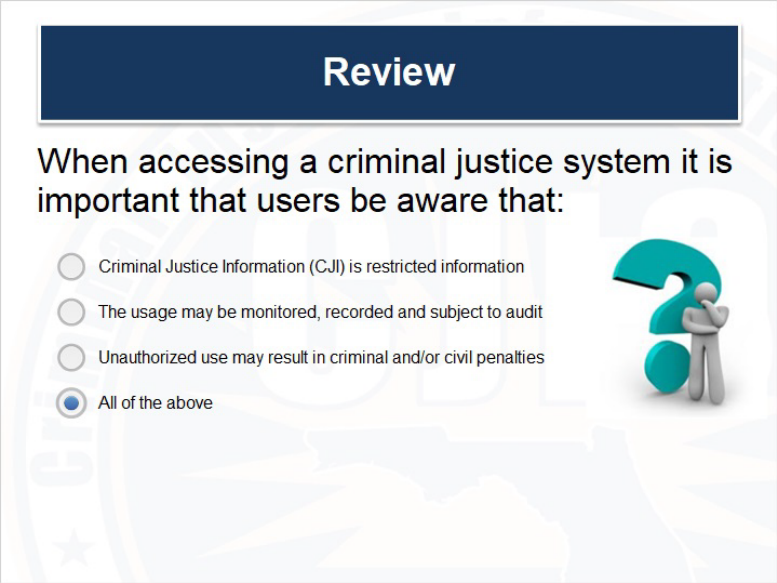
**Feedback when incorrect:**

You did not select the correct response.

## *Q1.11 Review Slide 11*

*(Multiple Choice, 10 points, unlimited attempts permitted)*

---




| Correct | Choice |
|---|---|
| | Criminal Justice Information (CJI) is restricted information |
| | The usage may be monitored, recorded and subject to audit |
| | Unauthorized use may result in criminal and/or civil penalties |
| X | All of the above |

**Feedback when correct:**

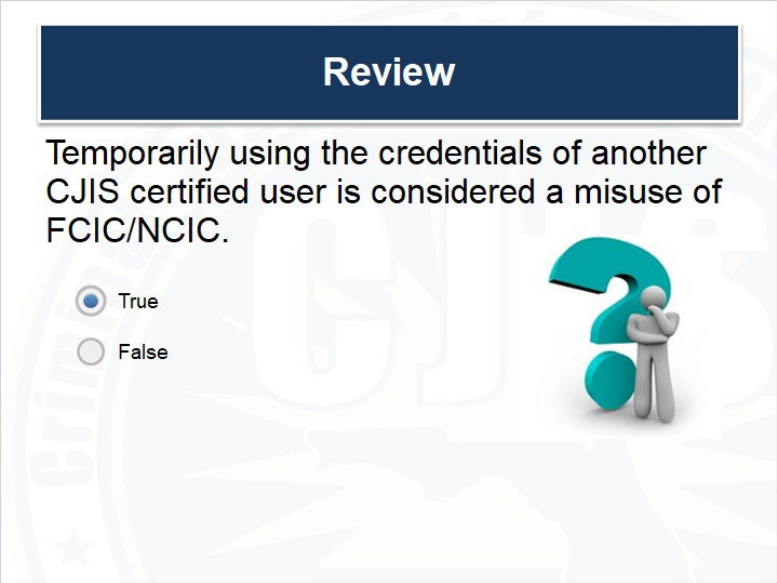
That's right!  CJI is restricted, usage is monitored, and misuse may result in penalties.

**Feedback when incorrect:**

You did not select the correct response.

## *Q1.12 Review Slide 12*

*(True/False, 10 points, 2 attempts permitted)*




| Correct | Choice |
|---|---|
| X | True |
| | False |

**Feedback when correct:**

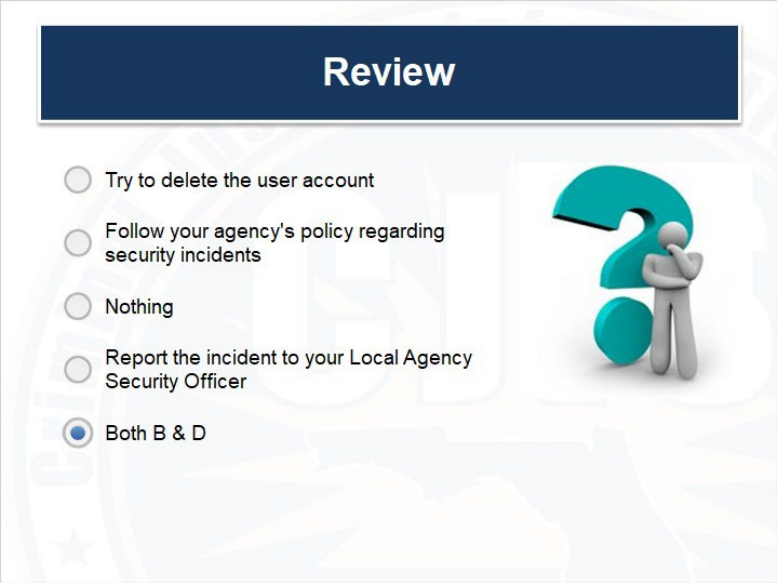
That's right!  Any unauthorized access of CJI is a misuse.

**Feedback when incorrect:**

You did not select the correct response.

## *Q1.13 Review*

*(Multiple Choice, 10 points, unlimited attempts permitted)*




| Correct | Choice |
|---|---|
| | Try to delete the user account |
| | Follow your agency's policy regarding security incidents |
| | Nothing |
| | Report the incident to your Local Agency Security Officer |
| X | Both B & D |

**Feedback when correct:**

That's right!  Always  follow agency policy and report suspicious activity.

**Feedback when incorrect:**

You did not select the correct response.