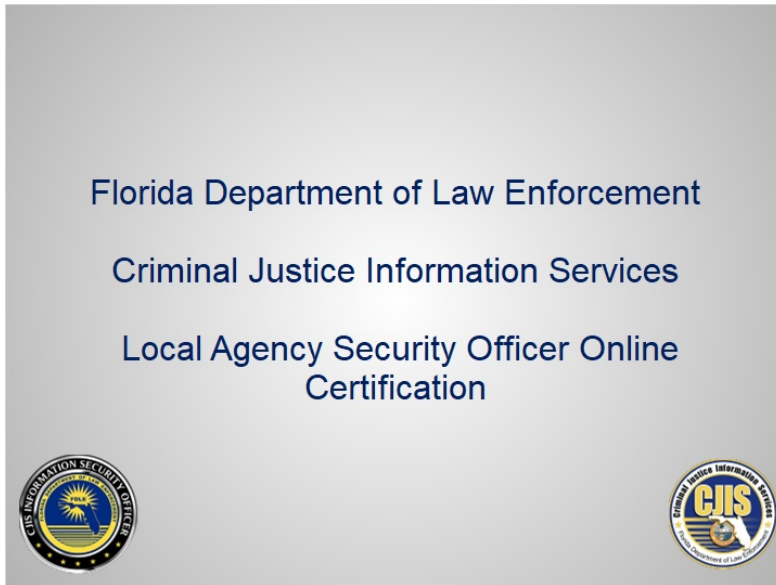


# Non Crim LASO Online Training V5

## 1. Local Agency Security Officer Training

### 1.1 Home Menu



**Notes:**

## 1.2 Slide 2 of 22

Welcome to the Florida Department of Law Enforcement Criminal Justice Information Services Local Agency Security Officer Training. This online training has a written and an audio component as well as a resources tab located at the top of the player, which lists useful items mentioned throughout this training. Please allot one hour to complete this training. Please click the LASO icon in the bottom right corner to ensure your audio is working.



### Notes:

Welcome to the Florida Department of Law Enforcement Criminal Justice Information Services Local Agency Security Officer Training. This online training has a written and an audio component as well as a resources tab located at the top of the player, which lists useful items mentioned throughout this training. Please allot one hour to complete this training. Please click the LASO icon in the bottom right corner to ensure your audio is working.

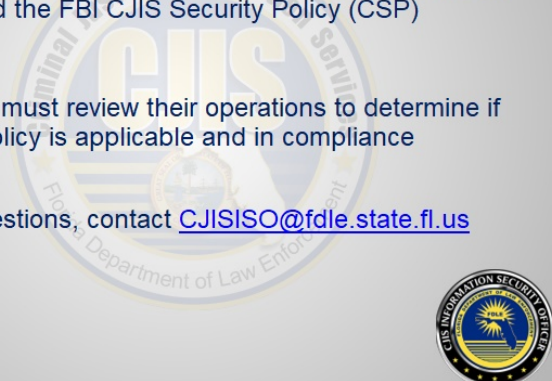
### 1.3 Slide 3 of 22

**GOAL**

Familiarize the Local Agency Security Officer (LASO) with the duties required by the FDLE User Agreement (UA) and the FBI CJIS Security Policy (CSP)

Agencies must review their operations to determine if policy is applicable and in compliance

For questions, contact [CJISISO@fdle.state.fl.us](mailto:CJISISO@fdle.state.fl.us)

The slide features a large, faint watermark of the FBI Seal and the Florida Department of Law Enforcement Seal in the background. In the bottom right corner, there is a smaller, official seal of the Florida Department of Law Enforcement, Information Security Officer.

#### Notes:

The goal of this training is to familiarize the Local Agency Security Officer (LASO) with the duties required by the FDLE User Agreement (UA) and the FBI CJIS Security Policy (CSP).

Please note: This training does not cover every issue within the CSP, but emphasizes certain areas. Agencies must review their operations and compare them with the requirements of the CSP and UA to determine if policy is applicable and is in compliance.

For questions, contact the FDLE CJIS Information Security Officer at the following email address: [CJISISO@fdle.state.fl.us](mailto:CJISISO@fdle.state.fl.us)

## 1.4 Slide 4 of 22


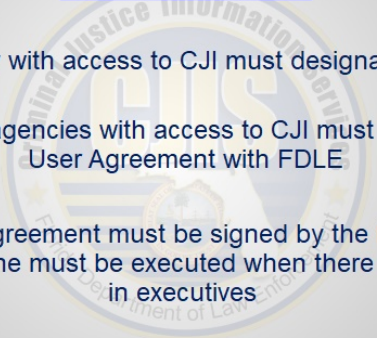
**INTRODUCTION**

A copy of the current FBI CSP can be located at  
[NCJA Resource Page](#)

Any agency with access to CJI must designate a LASO

All NCJA agencies with access to CJI must execute a  
User Agreement with FDLE

The User Agreement must be signed by the NCJA CEO  
and a new one must be executed when there is a change  
in executives



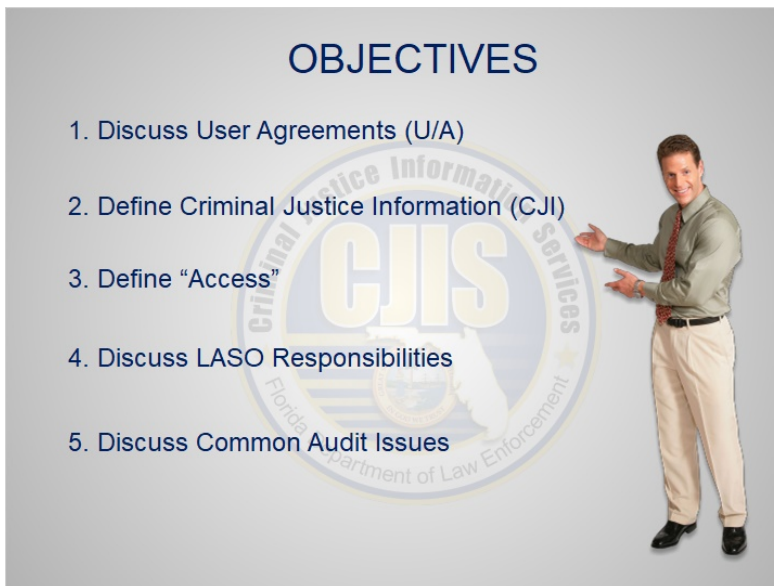
### Notes:

FDLE has adopted the FBI CSP as the standard for protecting Florida's Criminal Justice Information (CJI), a current copy of this document can be found on the Non Criminal Justice Agency (NCJA) Resource page located at the following link:  
<http://www.fdle.state.fl.us/NCJA-CSP-Compliance/Home.aspx>

The CSP [3.2.2] directs the CJIS Systems Officer (CSO) to ensure that any agency with access to CJI designate a Local Agency Security Officer (LASO).

FDLE is required by the CSP [5.1.1.6] to execute a User Agreement (UA) with each NCJA that is authorized to submit fingerprint based record checks and receive CJI. The UA identifies requirements the agency must follow to receive CJI and should be signed by the CEO of the NCJA. Agencies are asked to execute a new UA when there is a change in executives so as to familiarize the new administrator with the requirements pertaining to CJI access. The UA is periodically updated by FDLE depending on statute and policy changes.

## 1.5 Slide 5 of 22



**OBJECTIVES**

1. Discuss User Agreements (U/A)
2. Define Criminal Justice Information (CJI)
3. Define "Access"
4. Discuss LASO Responsibilities
5. Discuss Common Audit Issues

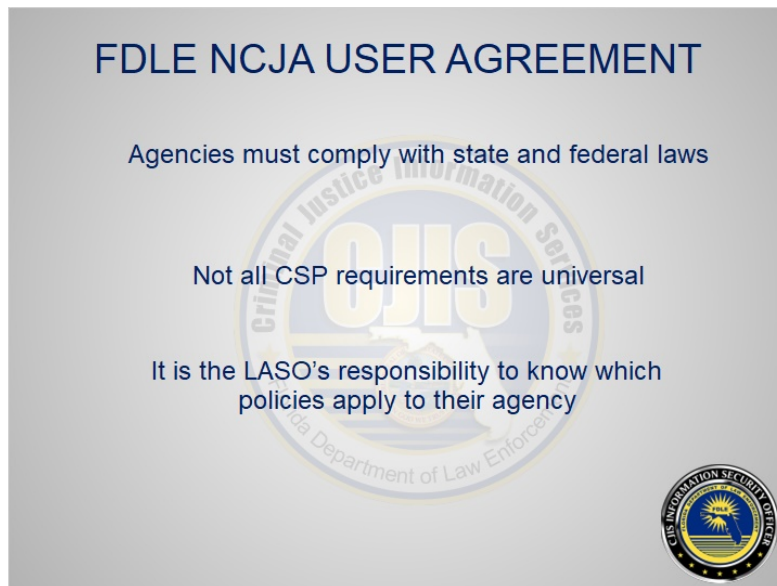
A man in a light green shirt and khaki pants stands to the right of the list, pointing towards the objectives. In the background, there is a large, faint watermark of the Florida Department of Law Enforcement (FDLE) seal, which includes the text 'Criminal Justice Information Services' and 'CJIS'.

### Notes:

The objectives of this course are to:

1. Discuss User Agreements (U/A)
2. Define Criminal Justice Information (CJI)
3. Define "Access"
4. Discuss LASO Responsibilities
5. Discuss Common Audit Issues

## 1.6 Slide 6 of 22



### Notes:

The FDLE NCJA User Agreement mandates agencies are subject and must comply with pertinent state and federal laws relating to the obtaining, use, and dissemination of records and record information derived from the systems of FDLE and the United States Department of Justice. This includes the agency's need to comply with the FBI CJIS Security Policy (CSP).

Some of the requirements in the CSP are universal and apply to all agencies; some apply to agencies that operate in certain IT configurations.


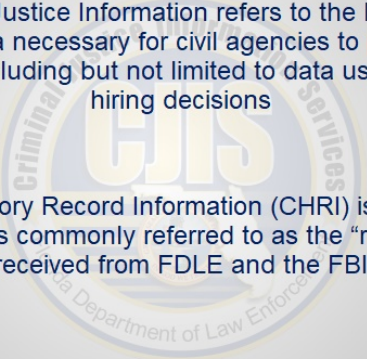
The agency LASO should know which requirements apply to his/her agency. As always, if there are questions, contact the FDLE CJIS ISO.

## 1.7 Slide 7 of 22

### Criminal Justice Information (CJI)

Criminal Justice Information refers to the FBI CJIS-provided data necessary for civil agencies to perform their mission; including but not limited to data used to make hiring decisions

Criminal History Record Information (CHRI) is a subset of CJI and is commonly referred to as the “rapsheet” received from FDLE and the FBI



#### Notes:

Criminal Justice Information, commonly referred to as CJI, refers to the FBI CJIS-provided data necessary for civil agencies to perform their mission; including, but not limited to data used to make hiring decisions. Criminal History Record Information (CHRI) is a subset of CJI, and is commonly referred to as the “rapsheet” received from FDLE and the FBI. For non-criminal justice agencies, the criminal history result from FDLE and the FBI when a fingerprint-based background check is completed is considered CJI, and must be protected.

## 1.8 Slide 8 of 22


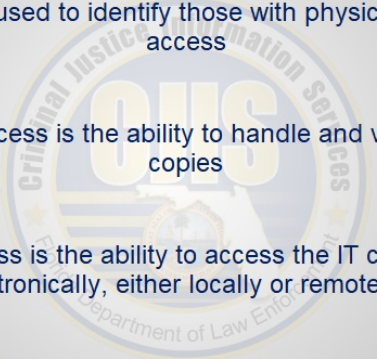
### WHAT DOES ACCESS TO CJI MEAN?

“Access” is used to identify those with physical or logical access

Physical Access is the ability to handle and view printed copies

Logical Access is the ability to access the IT component electronically, either locally or remotely

\*\*\*People have access through many different methods\*\*\*



#### Notes:

What does “access” to CJI mean?

“Access” is used to identify individuals who can physically or logically interact with CJI. If the agency does not store the information electronically on a computer or server in their office, logical access does not apply.

Physical access means the ability to handle and view printed copies.  
Logical access is the ability to access the IT component electronically, either locally or remotely.

Remember - People have “access” to CJI through many different methods. If there is a question regarding “access”, contact the FDLE CJIS ISO.



## 1.9 Slide 9 of 22



### Notes:

The next portion of this training will discuss the responsibilities of the LASO, which include

- Identify and Document Equipment
- Personnel Security (Security Awareness Training)
- Ensure Approved and Appropriate Security is in Place
- Outsourcing
- Protecting CJI
- Identify and Prevent Unauthorized Access
- Support Compliance and Notify Security Officer Promptly of Security Incidents

## 1.10 Slide 10 of 22

**LASO**

Does not have to be a technical person, but should have the authority to work with technical support personnel

Cannot be employed by a vendor

Extremely familiar with the security requirements of the UA and CSP

Know where to go in the CSP regarding security related issues

Must complete appropriate LASO training made available by FDLE on the CJIS Launch Pad within 2 Months of appointment

<https://florida.cjisapps.com/noncrim/launchpad>



### Notes:

The LASO:

The LASO does not have to be a technical person, but should have the authority to work with technical support personnel to ensure compliance with the UA and CSP. The LASO should be an employee of the NCJA. The LASO cannot be employed by a vendor.

The LASO should be extremely familiar with the security requirements of the UA and CSP and should know where to go in the CSP regarding security related issues. Within two months of appointment, the LASO is required to complete any appropriate LASO training made available by FDLE including security awareness training.


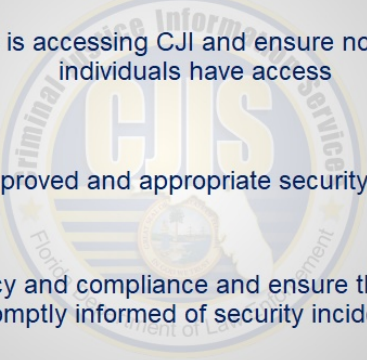
Resources to complete all CJIS training can be found on the CJIS Launch Pad located at the following link <https://florida.cjisapps.com/noncrim/launchpad>. The LASO should have a printed copy of the CSP that is easily accessible and become familiar with all the requirements that apply to your agency.

### **1.11 Slide 11 of 22**

**LASO Cont.**

LASO Shall:

- Identify who is accessing CJI and ensure no unauthorized individuals have access
- Ensure approved and appropriate security is in place
- Support policy and compliance and ensure the CJIS ISO is promptly informed of security incidents



#### **Notes:**

The FBI CSP defines specific duties that each LASO shall complete.

- Identify who is accessing CJI and ensure no unauthorized individuals or processes have access.
- Ensure the approved and appropriate security measures are in place and working as expected.
- Support policy compliance and ensure the CJIS ISO is promptly informed of security incidents.

## 1.12 Slide 12 of 22

**IDENTIFY AND DOCUMENT EQUIPMENT**


Both the UA and CSP [5.7 1.2] requires a network diagram in current status

LASO not specifically required to maintain diagram, but must produce it upon request

Not all agencies have the same diagram

FDLE requires current diagram when an agency is being audited

Does not have to document each device with access to CJI



### Notes:

#### Identify and Document Equipment

If electronic storage is used by an agency, a current network diagram shall be maintained. Both the UA and CSP [5.7.1.2] require agencies to keep a network diagram in current status.

The LASO specifically is not required to maintain the diagram, but must be able to produce the diagram upon request from FDLE or the FBI.

Some agencies will have very simple diagrams, others will be extremely complex.

FDLE will require a current network diagram when an agency is being audited.

The network diagram does not have to document each individual computer/device with access to CJI. It must identify any connections to other agency networks, the Internet and the firewalls protecting those connections.


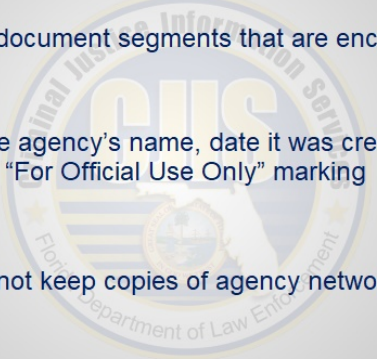
### 1.13 Slide 13 of 22

**IDENTIFY AND DOCUMENT  
EQUIPMENT Cont.**

Must document segments that are encrypted

Must include agency's name, date it was created, and a  
"For Official Use Only" marking

FDLE does not keep copies of agency network diagrams



#### Notes:

##### **Identify and Document Equipment**

Additionally, the network diagram must document those segments that are encrypted when information leaves the authorized facility and to the level to which the segment is encrypted.

The network diagram must include the agency's name, the date it was created/updated and a "For Official Use Only" marking.

FDLE does not keep copies of an agency's network diagram. If questions arise, FDLE will request the agency provide a copy for review.

## 1.14 Slide 14 of 22

**SECURITY AWARENESS TRAINING**

Anyone accessing CJI or using IT components to maintain CJI must take Security Awareness Training every 2 years

Level 1: Unescorted access to a physically secure location but do not deal directly with CJI

Level 2: Authorized personnel that have physical and/or logical access to CJI

Level 4: Any IT personnel



### Notes:

#### Security Awareness Training

All individuals who access or use CJI, or maintain IT components used to process or store unencrypted CJI must complete biennial (every two years) security awareness training.

Level 1 is for positions such as maintenance, custodial staff, and any other non-employees that have unescorted access to the CJIS physically secure location but do not deal directly with CJI.

Level 2 is for authorized personnel that have physical and/or logical access to CJI.

Level 4 is for any Information Technology personnel including IT vendors.

## 1.15 Slide 15 of 22


**ENSURE APPROVED  
AND APPROPRIATE  
SECURITY IS IN PLACE**

LASO is required to ensure both technical and non-technical compliance with CSP. LASO will oversee more technical areas such as:

- Information system audit logs
- Should pay particularly close attention to:
  - System access controls
  - Security Awareness Training
  - Remote access
- Outsourcing standards for Non-Channelers
- Media protection

**These are commonly cited compliance issues**

- Installation of newly released software such as firewalls, patches, spam, virus and spyware protections



### Notes:

#### **ENSURE APPROVED AND APPROPRIATE SECURITY IS IN PLACE**

Essentially, the LASO is required to ensure that the agency is in compliance with the CSP. This applies to both technical and non-technical policies. Although not specified in the UA or defined in the CSP as exclusively LASO duties, the LASO should pay particular attention to several other policy areas:

Security Awareness Training CSP [5.2]

Outsourcing Standards for Non-Channelers CSP[5.1.1.8]

These are not solely the responsibility of the LASO; however they are typically ones where agencies are cited for compliance issues.

The LASO doesn't have to personally take care of the duties, but should act as the focal point for the agency to assure their initial and ongoing integrity. In most agencies the LASO will oversee compliance with the more technical areas such as information system audit logs, system access controls, remote access, media protection as well as use of firewalls, prompt installation of newly released software security patches, spam, virus and spyware protections.

Again, it is strongly suggested that the LASO have a printed copy of the current CSP, highlighted and annotated ready for reference.

The LASO will be the primary contact during an FBI Information Technology Security

Audit and FDLE Technical Audit. Additionally, the FDLE Information Security Officer will reach out to the LASO regarding agency security issues.





## 1.16 Slide 16 of 22

### OUTSOURCING

Must be approved by CJIS Director and submitted to FDLE  
Example of contractors and vendors who have access to CJIS include:

- Maintenance of the network that stores CJI
- Storage facility providing space to store
- Shred company for destruction outside of the authorized agency



#### Notes:

Many non-criminal justice agencies are “outsourcing” certain functions. In many cases, the agencies are requiring these changes due to shrinking resources.

All criminal justice information administrative functions that are outsourced must be approved by the CJIS Director before entering into a binding contract with the vendor/contractor. Requests shall be submitted to FDLE, addressed to the CJIS Director on agency letter head, and signed by the agency head. Should you have any questions regarding this process please contact the CJIS ISO.

Example of contractors and vendors who have access to CJI can be, but not all inclusive, of the following:

Maintenance of the network that stores CJI;

Storage facility providing space to store CJI


Shred company for destruction outside of the authorized agency

## 1.17 Slide 17 of 22

### PROTECTING CJI

Agencies shall designate an area, room or storage container as a controlled area for the purpose of CJI:

- Limit access during CJI processing times
- Lock the area when unattended
- Position information containing CJI to prevent unauthorized individuals from access and view
- Follow encryption requirements when data is transmitted or stored outside of the authorized facility



#### Notes:

#### Protecting CJI

Agencies shall designate an area, a room or a storage container, as a controlled area for the purpose of day to day CJI access or storage [5.9.2]. This should include:

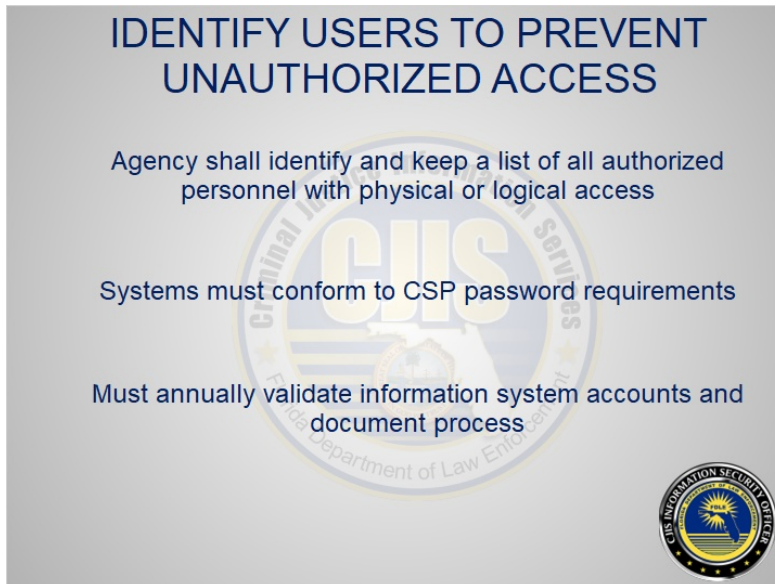
Limit access to the controlled area during CJI processing times to only those personnel authorized by the agency to access or view CJI.

Lock the area, room or storage container when unattended.

Position information system devices and documents containing CJI in such a way as to prevent unauthorized individuals from access and view.

Follow the encryption requirements found in Section 5.10.1.2 for electronic storage of CJI when data is transmitted or stored outside of the authorized facility.

## 1.18 Slide 18 of 22



**IDENTIFY USERS TO PREVENT UNAUTHORIZED ACCESS**

- Agency shall identify and keep a list of all authorized personnel with physical or logical access
- Systems must conform to CSP password requirements
- Must annually validate information system accounts and document process

The slide features a large, faint background watermark of the Florida Department of Law Enforcement (FDLE) seal. In the bottom right corner, there is a smaller, official seal of the Florida Department of Law Enforcement, Information Security Office.

### Notes:

The agency shall identify and keep a current list of all authorized personnel that have physical or logical access to the CJI data/systems, services and/or applications.

Systems that process or store CJI must conform to password requirements [5.6.2.1]. This is an often cited audit criticism. This applies to all systems and/or applications that process or store CJI.

Additionally, each agency is required to annually validate information system accounts, and document that process [5.5.1]. Again, this applies to all systems containing CJI.

## 1.19 Slide 19 of 22

**SUPPORT COMPLIANCE AND NOTIFY CJIS ISO PROMPTLY OF SECURITY INCIDENTS**


LASO must inform the FDLE CJIS ISO of any security incidents

Each agency must have security response policy

Employees must know what actions to take in the event of a suspected computer security incident

The LASO should notify the FDLE CJIS ISO via email [CJISISO@fdle.state.fl.us](mailto:CJISISO@fdle.state.fl.us) and the Customer Support Center: [FDLECustomerSupport@fdle.state.fl.us](mailto:FDLECustomerSupport@fdle.state.fl.us)

[Security Incident Response Form](#)



### Notes:

Support Compliance and Notify CJIS ISO Promptly of Security Incidents

A primary role of the LASO is to inform the FDLE CJIS ISO of any security incidents.

Each agency must have a security incident response policy/program. The size and complexity of the policy will vary from agency to agency based on the size and complexity of the agency and network.

Employees must know what actions to take in the event of a suspected security incident, particularly who to notify.

The LASO, once notified of a possible security incident, should notify via email the FDLE CJIS ISO [CJISISO@fdle.state.fl.us](mailto:CJISISO@fdle.state.fl.us) AND Customer Support Center [FDLECustomerSupport@fdle.state.fl.us](mailto:FDLECustomerSupport@fdle.state.fl.us). The email should be marked with a "High" importance. A sample of a response form can be found at the link below:

<http://www.fdle.state.fl.us/NCJA-CSP-Compliance/Documents/SecurityIncidentResponseForm-NCJA-022018.aspx>

## 1.20 Slide 20 of 22


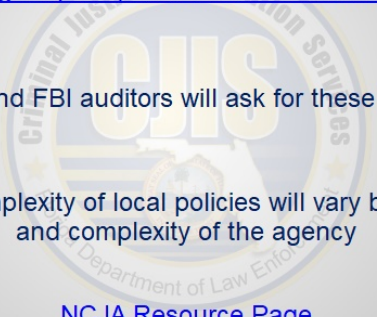
**REQUIRED POLICIES**

The required policies checklist can be found at:  
[Agency Required Policies Checklist](#)

FDLE and FBI auditors will ask for these policies

Size and complexity of local policies will vary based on size  
and complexity of the agency

[NCJA Resource Page](#)



### Notes:

#### Required Policies

Finally, throughout the CSP there are a number of local policies that are required. FDLE has created a “checklist” to identify those policies and where each is cited in the CSP.

The checklist can be found at:

<http://www.fdle.state.fl.us/NCJA-CSP-Compliance/Documents/AgencyRequiredPolicyChecklistNCJA.aspx>

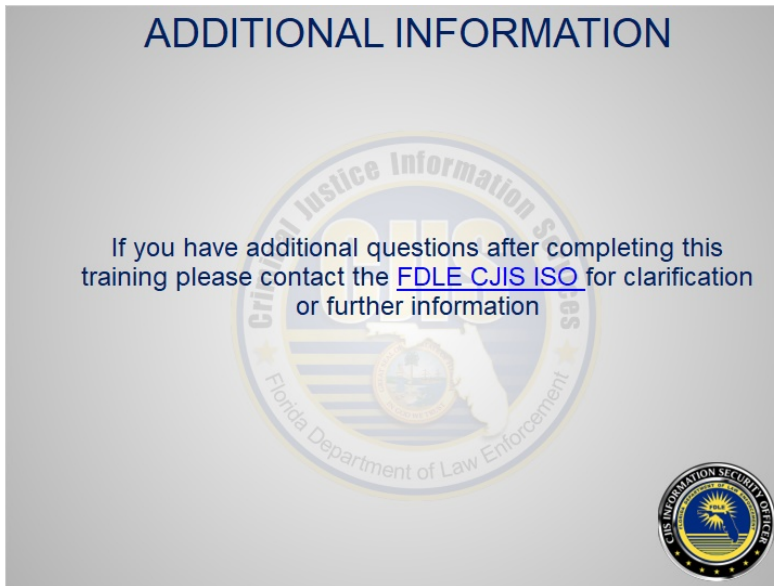
FDLE and FBI technical auditors will ask for these policies.

Again, the size and complexity of local policies will vary from agency to agency based on the size and complexity of the agency and network, as well as business operations.

Sample policies can be found on the NCJA Resource Page at the below link:

<http://www.fdle.state.fl.us/cms/NCJA-CSP-Compliance/Resources.aspx>

## 1.21 Slide 21 of 22



### Notes:

Once more, this training is designed to broadly highlight LASO duties identified in the CJIS Security Policy and the FDLE Non Criminal Justice User Agreement. No two agencies operate or manage their administration of criminal justice information in the same manner. As such, this training is not designed to answer all questions, but will most likely generate additional questions.

Please contact the FDLE CJIS ISO at [CJISISO@fdle.state.fl.us](mailto:CJISISO@fdle.state.fl.us) for additional information.

## 1.22 Slide 22 of 22

**TRAINING CONFIRMATION**

You have completed the LASO Online Training. Please click the Information Security Officer Logo below to exit the course and return to nexTEST.



The logo is circular with a blue border. Inside the border, the text "Criminal Justice Services" is written in a semi-circle at the top and "Florida Department of Law Enforcement" is written in a semi-circle at the bottom. In the center of the logo is a smaller circle containing a sun rising over a road, with the text "CIS INFORMATION SECURITY OFFICER" around it.

You may begin the LASO exam immediately, or you may return within fourteen (14) days to complete the exam.

### Notes:

You have completed the LASO Online Training. Please click the Information Security Officer Logo below to be redirected to the nexTEST login page.

You may begin the LASO exam immediately, or you may return within fourteen (14) days to complete the exam.