Local Agency Security Officer (LASO) Training

Florida Department of Law Enforcement

Criminal Justice Information Services

January 2017

This training is designed to familiarize the Local Agency Security Officer (LASO) with the duties required by the FDLE User Agreement (U/A)and FBI CJIS Security Policy (CSP).

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 U/A to determine if policy is applicable and is in compliance.

When questions arise, contact the FDLE CJIS ISO – HarryLaine@fdle.state.fl.us.

The LASO should have a printed copy of the CSP. A copy of the current FBI CSP can be found on the NCJA Resource Page located at:

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

Go through the CSP and highlight each “Shall”. These are the required policies within the CSP. FDLE and the FBI will audit the “Shall” statements. Also, this process will help familiarize the LASO with the CSP.

Not all “Shall” statements will apply to each agency. Any questions about whether a “Shall” statement applies to an agency should be directed to the FDLE CJIS ISO – HarryLaine@fdle.state.fl.us.

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 U/A and CSP.

The LASO should to be extremely familiar with the security requirements of the U/A and CSP. The LASO should know where to go in the CSP regarding security related issues.

The LASO should regularly check the NCJA Resource Page for updates, changes and new information at: http://www.fdle.state.fl.us/NCJA-CSP-Compliance/Resources.aspx

In this training, CSP referenced are bracketed, e.g., [5.6.2.2] while the U/A references are in parenthesis (Section II, para 1).

Access to Criminal Justice Information (CJI)

Throughout this training and the CSP, the term “access” is used to identify individuals who need to go through security awareness training. Sometimes the term “physical or logical access” is used.

Physical access is the ability to physically “touch” the IT component, unplug the power cable at the device, push a power button on the device, connect a USB flash drive to a port, plug or unplug a network cable, etc. This is not an all inclusive list, but an overall idea regarding physical access. Depending on the layout, hardware locked in a cabinet can be protected from physical access.

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.

FDLE has adopted the FBI CJIS Security Policy (CSP) as the standard for protecting Florida's Criminal Justice Information (CJI).

The FDLE NCJA User Agreement mandates "agencies are subject and must comply with pertinent state and federal regulations 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 (Section I (2))". This includes the agency right 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.

Each entity with access to the fingerprint-based background check is required to execute a User Agreement (U/A) with FDLE.

FDLE strongly recommends within six months of assignment to the position, the LASO is encouraged to complete any appropriate LASO training made available by FDLE, including CJIS security awareness training.

The LASO shall ensure the security of:

- The workstations;
- The access to the information services provided. These

duties are part of the CSP requirements for the LASO **[3.2.9]**.

The FBI CJIS Security Policy (CSP) defines specific duties that each LASO shall complete [3.2.9]:

1. Identify who is using the CSA (FDLE is the CJIS Systems Agency for Florida) approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access.
2. Ensure that personnel security screening procedures (security awareness training) are being followed as stated in this policy (the CSP).
4. Ensure the approved and appropriate security measures are in place and working as expected.
5. Support policy compliance and ensure CSA CJIS ISO (Harry Laine) is promptly informed of security incidents.

The remaining part of this training will expand on these duties.

1. Identify and Document Equipment

Each agency must maintain a current network diagram. The CSP [5.7.1.2] requires 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 and the Internet and the firewalls protecting those connections.

1. Identify and Document Equipment (cont.)

Additionally, the network diagram must document those segments that are encrypted and 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.

2. Personnel Security (Security Awareness Training)

Each agency shall properly administer the FDLE provided security awareness training (CJIS Online) to all agency personnel with access to CJI.

Access includes those individuals who have unescorted access to the CJI, maintain systems used to process or store unencrypted CJI or have unescorted access in a physically secure location as defined in CSP [5.9.1]. This Includes vendors, support personnel or custodial staff.

FDLE requires that the basic security awareness shall be required within six months of initial assignment for employees, prior to granting access to non-employees, and biennially thereafter.

Although not specified in the U/A 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]
- Information Exchange Agreements [5.1.1.4]
- Outsourcing Standards for Non-Channelers CSP [5.1.1.8]
- Physically Secure Location CSP [5.9.1]

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

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.

The CSP requires three different levels of training based on the type of access of the user: Level 1 - baseline (contact), Level 2 - those with physical/logical access (hear or read), and Level 4 - those in an IT role (fixers).

Information Exchange Agreements

Overall FDLE User Agreement

FDLE is required by statute (943.05(2), F.S.) and the CSP [5.1.1.3] to execute a user agreement (U/A) with each agency that accesses CJI. The U/A identifies requirements the agency must follow to access CJI and is usually signed by the CEO of the non-criminal justice agency. Agencies are asked to execute a new U/A when there is a change of executives so as to familiarize the new administrator with the requirements pertaining to CJI access. The U/A is periodically updated by FDLE depending on statute and policy changes.

Between Agencies

Information Exchange Agreements outline the roles, responsibilities, and data ownership between agencies and any external parties. Information Exchange Agreements for agencies sharing CJI data that is sent to and/or received from the FBI CJIS shall specify the security controls and conditions described in this document [5.1.1].

Information exchange agreements shall be supported by documentation committing both parties to the terms of information exchange. As described in subsequent sections, different agreements and policies apply, depending on whether the parties involved are CJAs or NCJAs. See Appendix D in the CSP for examples of Information Exchange Agreements.[5.1.1]

Outsourcing

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 (Charles Schaffer) 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.

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

- IT vendor providing services of the hardware, software, or firmware to the agency network that obtains unencrypted CJI;
- Storage facility providing space to store CJI in unsecured boxes.

As always, if there are questions, contact the FDLE CJIS ISO.

Outsourcing (cont.)

In both situations, where the Outsourcing Standard applies, the Non-Criminal Justice Agency (NCJA) will be performing security awareness training on all personnel who have unescorted physical or logical access to systems that process CJI. This includes custodial staff or contractors with physical access.

Those members who maintain IT components that process or store CJI, including remote access, are required to complete security awareness training as well.

Private Contractor for NCJA (Governmental)

Private contractors designated to perform criminal justice functions on behalf of a NCJA (government) shall be eligible for access to CJI. Access shall be permitted only if an agreement is in place specifically identifying the agency's purpose and scope of providing services for the administration of criminal justice.

The agreement between the NCJA and the private contractor shall incorporate the CJIS Security Addendum approved by the Director of the FBI, acting for the U.S. Attorney General, as referenced in Title 28 CFR 20.33 (a)(7). [5.1.1.5 (2)].

Security Addendum

A NCJA (government) may outsource a criminal justice function to a private entity. To allow the private entity the ability to “access” CJI, the contract for outsourcing must include/incorporate the FBI Security Addendum (see Appendix H of the CSP).

As part of the Security Addendum process, each employee of the private entity with access to CJI must complete the required security awareness training and sign the Certification Page of the Security Addendum. The certification pages must be kept by the NCJA for audit review.

Physically Secure Location (PSL) (cont.)

The CSP defines the requirements for a PSL [5.9.1.1-5.9.1.9]. The wording of the requirements is broad. It was designed that way to help smaller agencies meet physical security requirements without placing a great strain on resources.

Most agencies already comply with these requirements for physical security. In some cases, agencies will need to review the physical layout with FDLE to determine compliance.

There will be instances where the agency cannot meet the requirements of a PSL, but still has the operational need to access CJI. In those situations the area can be designated a “Controlled Area” [5.9.2].

Two of the primary requirements of a controlled are: electronic storage of CJI must be encrypted and lock the area or storage container when unattended.

3. Ensure Approved and Appropriate Security is in Place

This is the “catch all” clause of the LASO duties. Essentially, this one means that the LASO will ensure that the agency is in compliance with the CSP. This applies to both technical and non-technical policies.

Again, the LASO doesn’t have to personally take care of the duties, but should act as the focal point for the agency to assure the initial and ongoing integrity of the system. In most agencies the LASO will oversee compliance with the more technical area 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 for ready reference.

The LASO will be the primary contact during an FBI Information Technology Security Audit and FDLE Technical Audit. Additionally, the FDLE ISO will reach out to the LASO regarding agency security issues.

4. Identify users to prevent unauthorized access (cont.)

The agency shall identify and keep a current list of all authorized personnel that has 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.

5. Support Compliance and Notify CSA 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 shall notify via email the FDLE CJIS ISO fdlecjisiso@fdle.state.fl.us ***AND*** Customer Support Center FDLECustomerSupport@fdle.state.fl.us. The email should be marked with a "High" importance. A copy of the response form can be found on the NCJA Resource page under Information Security http://www.fdle.state.fl.us/NCJA-CSP-Compliance/Documents/SecurityIncidentResponseForm(201506).aspx

Required Policies

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

The checklist can be found at:

http://www.fdle.state.fl.us/NCJA-CSP-Compliance/Resources.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

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

Again, 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 their administration of criminal justice information in the same manner. As such, this training is not designed to answer all questions.

This training will most likely generate additional questions.

Please contact the FDLE CJIS ISO for clarification or further information.

If you are a LASO, when you have completed this PowerPoint presentation, please forward an acknowledgement email, with "LASO Training" in the subject line, to: HarryLaine@fdle.state.fl.us and your regional FDLE IDT representative.

Questions should be forwarded to the FDLE CJIS ISO:

Harry Laine

HarryLaine@fdle.state.fl.us