SPECIAL NOTE

LASO training is automated and online.
Training is now available @
https://www.cjisonline.com

Our team will continue to accept this paper method until we phase out this manual process.

Texas Department of Public Safety

CJIS Security Office

Information Security – LASO Training

07/08/2021

Texas Department of Public Safety

This training is designed to familiarize the Local Agency Security Officer (LASO) with the duties required by the FBI CJIS Security Policy (CSP).

This training does not cover every topic within the CSP, but emphasizes certain areas.

Agencies must review their operations and compare them with the requirements of the CSP to determine what is applicable and in compliance for their agency.

Texas Department of Public Safety

Agenda

- CJIS Security Policy requirements
- LASO role and responsibilities
- Focus topics for a LASO
- 2019 CSA Audit Results
- 2019 Texas Agencies Audit Summary
- Resources / Links

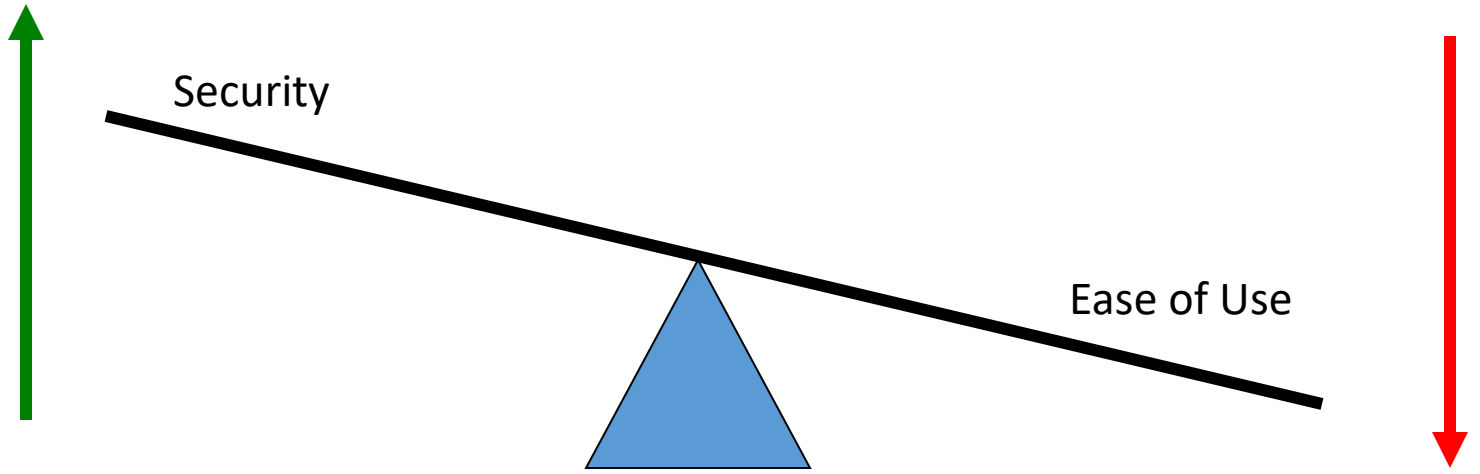
Texas Department of Public Safety

The CJIS Security Policy (CSP) provides the minimum level of Information Technology (IT) security requirements acceptable for the transmission, processing and storage of Criminal Justice Information Systems (CJIS) data.

Texas Department of Public Safety

There is always a conflict between Computer Security and how easy a computer is to use.

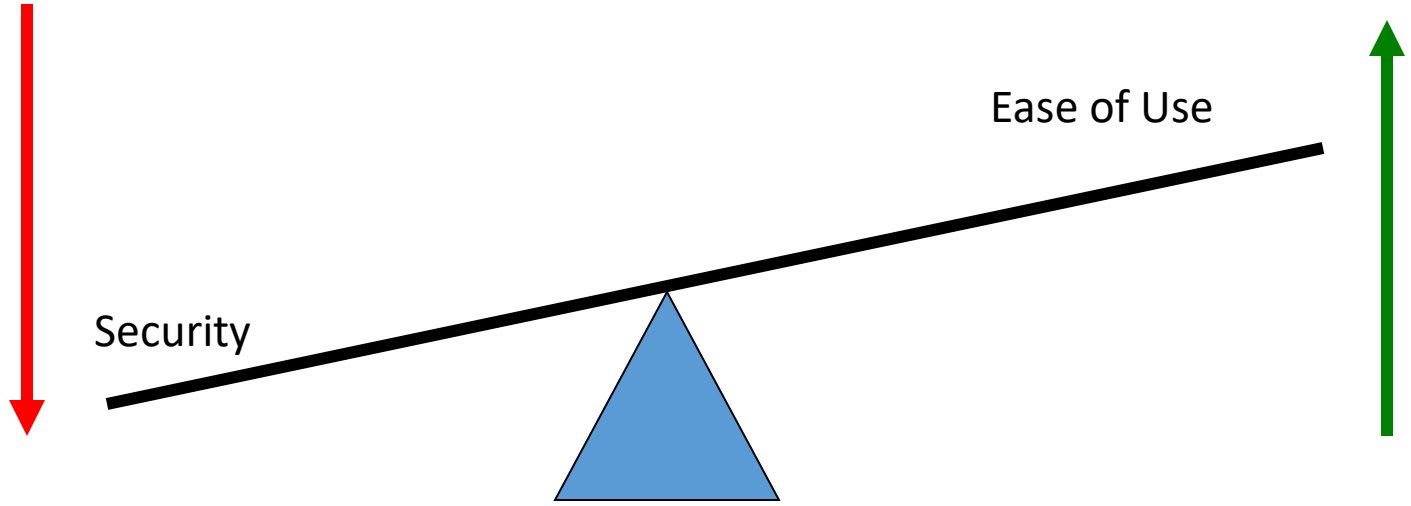
As Computer Security Increases, Ease of Use decreases.



Texas Department of Public Safety

The reverse is also true.

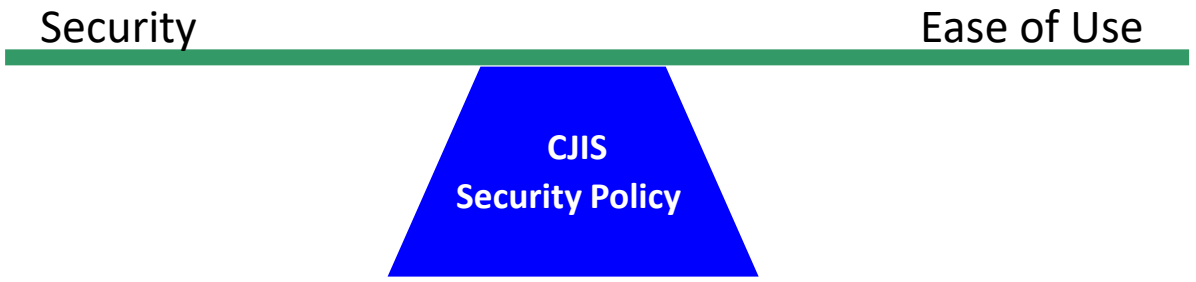
As Ease of Use Increases, Computer Security decreases.



Texas Department of Public Safety

A balance between Security and Ease of Use is needed.

The CJIS Security Policy provides a foundation that balances Security and Ease of Use.



Texas Department of Public Safety

The CJIS Security Policy defines:

- Roles and responsibilities:
  CSO, TAC, LASO
- Physical security requirements
- Technical security requirements
- Best Practices information (Appendices)

Texas Department of Public Safety

- CSO — CJIS Systems Officer
  (state level – Mike Lesko in Crime Records)
- CJIS ISO — CJIS Information Security Officer
  (state level – Stephen 'Doc' Petty in Crime Records)
- TAC — Terminal Agency Coordinator
  (point of contact at the local agency for TLETS access)
- LASO — Local Agency Security Officer

Texas Department of Public Safety

CJIS Policy defines LASO responsibilities as follows:

1. Identify who is using the CSA approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.

2. Identify and document how the equipment is connected to the state system.

3. Ensure that personnel security screening procedures are being followed as stated in this Policy.

4. Ensure the approved and appropriate security measures are in place and working as expected.

5. Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.

Texas Department of Public Safety

Becoming familiar with the CJIS Security Policy

The LASO should have access to a current copy of the CJIS Security Policy (CSP).

As an appointed LASO, go through the CSP and highlight each “Shall”. These are the required elements within the CSP. Audits are based upon these “Shall” statements.

This process will help familiarize the LASO with the CSP and the critical areas of focus.

Note: not all “Shall” statements will apply to each agency.

Texas Department of Public Safety

The LASO does not have to be a technical person, but should have the authority, and ability to work with technical support personnel to ensure compliance with the CSP.

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

The LASO should regularly check our web page for updates, changes and new information. Stay current on any changes or security trends which may impact Law Enforcement.

Texas Department of Public Safety

Technical Audits of CJIS Information Systems

Each CSA (TX DPS) shall establish a system to, at a minimum, triennially audit all criminal justice and noncriminal justice agencies which have direct access to the state system in order to ensure compliance with agency and FBI CJIS Division policy and regulations.

Texas Department of Public Safety

Shared Management Philosophy

In the scope of information security, the FBI CJIS Division employs a shared management philosophy with federal, state, local, and tribal law enforcement agencies.

The FBI has a similar relationship with the Compact Council, which governs the interstate exchange of criminal history records for noncriminal justice purposes.

Texas Department of Public Safety

The CJIS Security Policy contains information you need as an appointed LASO to protect Criminal Justice data and ensure the access is limited to only those personnel who have a need for, and are authorized to receive CJI.

There is additional “best practices” information in the appendices which may be useful in meeting your assigned responsibilities.

Texas Department of Public Safety

Focus Topics for a LASO

Physical Security (CSP 5.9) – without physical security no other security measures can be considered effective.

Personnel Security (CSP 5.5) – What do you know about those that have access?

Security Awareness Training (CSP 5.2) - Security is everyone's responsibility.

Disposal of Media (CSP 5.8) – Know how to correctly dispose of media (paper, discs, CD's, computers, note paper – anything + everything.)

Texas Department of Public Safety

Focus Topics for a LASO

Keep systems updated (CSP 5.10.4) – ALL hardware and software should be updated with the latest security releases.

Passwords (CSP 5.6) – Use strong passwords, use passwords you can remember. Never share – you are responsible for your User ID.

Use anti-virus software (CSP 5.10.4) – Use a brand-name, should always be running, MUST be kept updated.

Encryption (CSP 5.10.1.2) – If data is transmitted outside the secure area, it must be encrypted. Look for NIST certification to FIPS 140-2 standard.

Texas Department of Public Safety

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 network diagram must include the agency's name, current date and "For Official Use Only".

The LASO is responsible to ensure a current diagram is maintained, and must be able to provide the diagram upon request from TX DPS or the FBI.

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

TX DPS will always require a current network diagram when an agency is being audited.

Note: Network diagram samples are on our web page.

Texas Department of Public Safety

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

Validate vendors with remote access credentials.

Systems that process, transmit or store CJI must conform to password requirements (5.6.2). This applies to all systems and/or applications that process, transmit or store CJI.

Additionally, each agency is required to annually validate information system accounts, and document that process (5.5.1).

Texas Department of Public Safety

Ensure agency personnel and vendor personnel are fingerprint background cleared within the state of Texas at TCOLE standards before receiving *unescorted* physical or logical access to CJI systems (CSP 5.12).

Ensure agency personnel and vendor personnel receive the appropriate level of CJIS Security Awareness Training (CSP 5.2).

Ensure vendors with remote access have proper clearance, utilize FIPS 140-2 level remote access methods and have a second factor to authenticate for Advanced Authentication (AA) requirements.

Texas Department of Public Safety

Best Practices

- Periodically check to ensure Servers/Terminals/MDTs connected to the CJIS network are receiving the latest Operating System & Anti-virus software updates; ensure personal firewalls are enabled on MDTs; ensure System screens are locked with a screensaver within thirty (30) minutes on *non*-dispatch Terminals & MDTs.

- Periodically check physically secure location(s) to ensure safeguards such as locks are in working order; Doors are closed & properly secured; Terminals are not viewable by unauthorized personnel.

- Periodically check to ensure all network components (routers, firewalls, switches) processing CJIS information are still supported by the manufacturer. If warranties/contracts are in place, ensure they are valid and not out of date.

- Periodically check pertinent documents, Security Addendums, MCAs, etc., to ensure they are up to date. Take appropriate action such as making editing changes or replacement if required.

Texas Department of Public Safety

The LASO is required to help ensure the agency is in compliance with the CSP. This applies to both technical and non-technical policies.

The LASO must ensure security processes and practices are in line with meeting the requirements of the CSP for the local agency. The LASO acts as the focal point for the agency to assure the initial and ongoing integrity of the systems. 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.

Texas Department of Public Safety

Incident Response (IR)

A primary role of the LASO is to inform the TX DPS CJIS Security Office of any security incidents. Timely notification and response are key to securing the state's systems.

Each agency must have a security incident response policy. The size and complexity of the policy will vary from agency to agency based on the size and complexity of the agency and network. For assistance or samples of IR policies contact the TX DPS CJIS Security Team or review sample policies available on our website.

Employees must know what actions to take in the event of a suspected security incident, who to notify, and how. Ensure your local IR policy includes contact lists of key responders.

Incident first contact to OIC @ 1.800.638.5387 (1.800. 63.TLETS)

Texas Department of Public Safety

Online CJIS Security Technical Audit

Texas employs an online CJIS Audit, coupled with a follow up site visit and walkthrough. The online audit process provides the agency with any audit findings for compliance with the CJIS Security Policy and the ability to review past audits online.

As a LASO, be familiar with your assigned auditor(s). Work together with your local TAC to ensure you have access to review past audits or areas of concern.

Texas Department of Public Safety

FBI Findings 2019 Audit of State of Texas (CSA)

Texas Department of Public Safety (CSA) – The Mobile Biometric Identification System (MBIS) passwords did not expire within a maximum of 90 days and did not have a password history of at least ten previous passwords.

Texas Department of Public Safety

2019 FBI Audit Policy Compliance Summary for the State of Texas (Local Agency Findings)

Policy	Finding
System Administration	
CJIS Systems Officer (CSO)	**IN**
Information Security Officer (ISO)	**IN**
Local Agency Security Officer (LASO)	**IN**
Administration of Criminal Justice Functions	
Criminal Justice Agency User Agreements	**IN**
Information Exchange Agreements	**IN**
Management Control Agreements	**IN**
CJIS Security Addendums	**IN**
Agency Coordinator	**IN**
Management Control	**IN**

Texas Department of Public Safety

Information Protection	
IT Security Program	**IN**
Standards of Discipline	**IN**
Personnel Security	**IN**
Security Awareness Training	**IN**
Physical Security	**IN**
Security Audits	**IN**
Media Protection	**IN**
Media Transport	**IN**

Texas Department of Public Safety

Policy	Finding
Network Infrastructure	
Network Configuration	**IN**
Personally Owned Information Systems	**IN**
Publicly Accessible Computers	**IN**
System Use Notification	**IN**
Identification (ID)/UserID	**IN**
Authentication	**OUT**
Session Lock	**IN**
Event Logging	**OUT**
Advanced Authentication	**OUT**

Texas Department of Public Safety

Encryption	**IN**
Dial-up Access	**IN**
Mobile Devices	**IN**
Personal Firewalls	**IN**
Bluetooth Access	
Wireless (802.11x) Access	**IN**
Boundary Protection	**IN**
Intrusion Detection Tools & Techniques	**IN**
Malicious Code Protection	**IN**
Spam and Spyware Protection	**IN**
Security Alerts and Advisories	**IN**
Patch Management	**IN**
Voice over Internet Protocol (VoIP)	**IN**

Texas Department of Public Safety

Partitioning and Virtualization	**IN**
Cloud Computing	**IN**
Security Incident Response	**IN**

Texas Department of Public Safety

Resources & Links

FBI CJIS Security Policy: https://www.dps.texas.gov/SecurityReview/documents.htm

Fingerprint background access chart:
https://www.dps.texas.gov/SecurityReview/documents/tcicAccessPolicyChart.pdf

Security Awareness Training: https://www.dps.texas.gov/SecurityReview/secAwareness.htm

Forms, sample documents & network diagrams, listserv enrollment are available on the security review web site: https://www.dps.texas.gov/securityreview

Join the CJIS listserv https://www.dps.texas.gov/securityreview/AlertRegistration/default.aspx

Texas Department of Public Safety

After completing review of this LASO training document, please send an email with your name, agency name, agency ORI and date completed to:

security.committee@dps.texas.gov