



2022 CJIS LASO Training

Utah CJIS ISO

Introductions

Tyson Jarrett



Utah CJIS ISO - As of May 2022

12 years experience in Electrical Grid auditing and regulation (NERC)

Jarrel Beal



Utah CJIS Auditor - As of December 2021

7 years experience in auditing

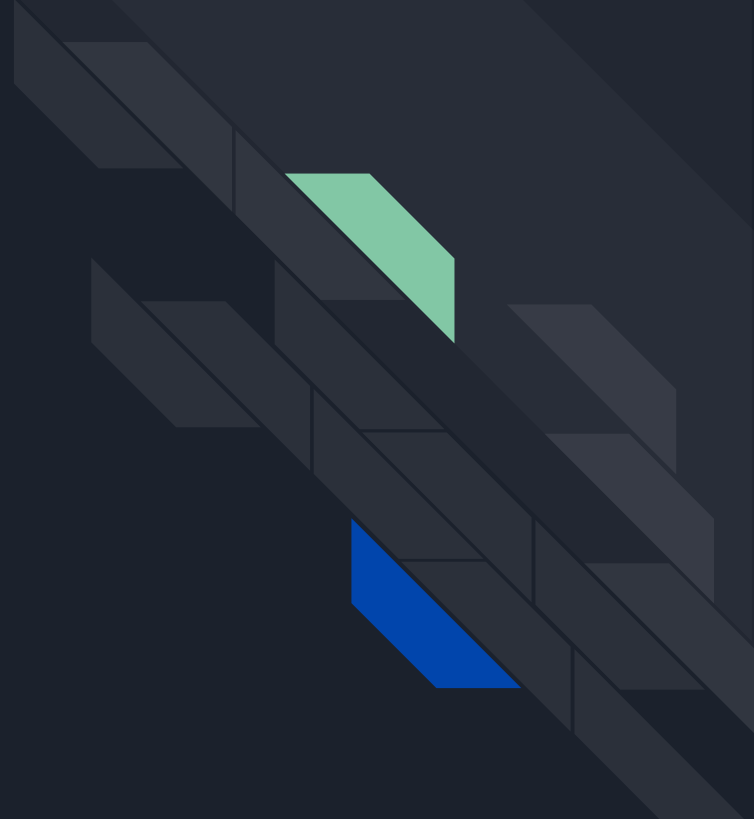


Purpose/Agenda

The CJIS Systems Agency (Utah Bureau of Criminal Investigation) is required to ensure each LASO receives enhanced security awareness training (CJIS Security Policy Section 3.2.2). Per the policy, the following topics shall be addressed as enhanced security awareness training:

1. The roles and responsibilities listed in CJIS Security Policy Section 3.2.9.
2. Additional state/local/tribal/federal agency LASO roles and responsibilities.
3. Summary of audit findings from previous state audits of local agencies.
4. Findings from the last FBI CJIS Division audit of the CSA.
5. Most recent changes to the CJIS Security Policy.

Local Agency Security Officer (LASO)





Roles and Responsibilities

Per the FBI CJIS Security Policy, every agency that has access to CJI is required to have an identified LASO who shall:

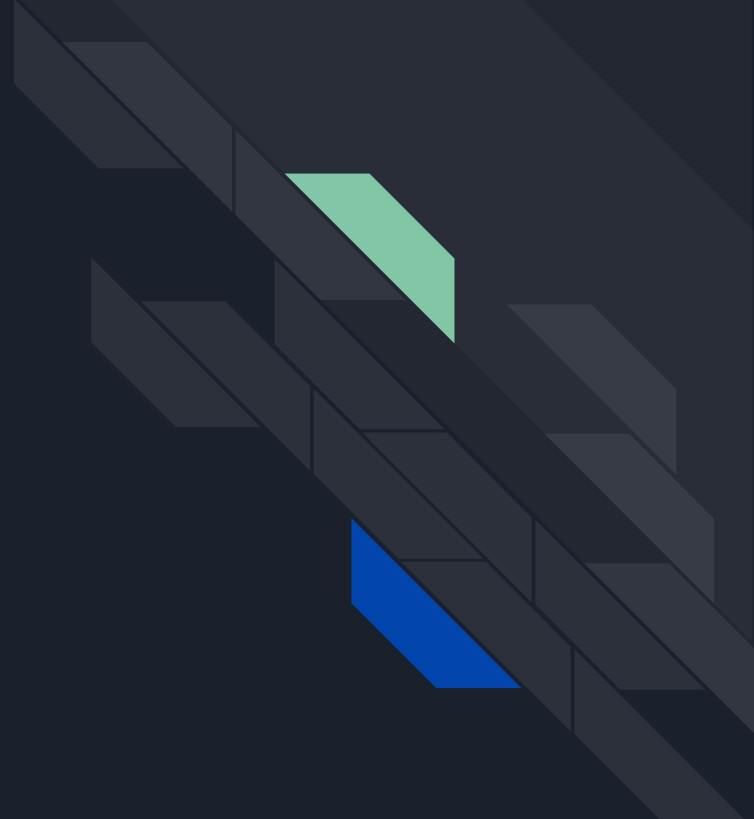
1. Identify who is using the CSA approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.
2. Identify and document how the equipment is connected to the state system.
3. Ensure that personnel security screening procedures are being followed as stated in the CJIS Security 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



Roles and Responsibilities (cont'd)

- Local agency TAC and LASO should work closely with each other to ensure communication of requirements and compliance standing.
- Typically the LASO will be the technical resource in a local agency's security program
- LASO is required to receive enhanced training on the specific duties and responsibilities of their position and the impact that position has on the overall security of information systems.
 - LASO training shall be encouraged prior to assuming duties but should not occur later than six months after initial assignment, and annually thereafter.
- The LASO actively represents their agency in all matters pertaining to Information Security, including:
 - Disseminating alerts and other material to their constituents
 - Maintaining documentation (including system configuration data)
 - Assisting with audits of hardware and procedures
 - Keeping the CSA informed on any needs or problems.

CJIS Audit Findings





CJIS Audit Findings

Policies not documented or not tailored to the agency


Agencies should have documented policies in place that align with the CJIS Security Policy (CSP). The most commonly insufficiently documented policies are:

1. Incident Response Plan (Usually copied from the CSP and/or doesn't detail the required procedures outlined in 5.3.2.1)
1. Media Protection Policy (Usually missing procedures associated with the access, transport, storage, and sanitization of physical & digital CJI)
1. Physical Protection Policy (Usually missing procedures associated with physical access authorizations, control, and monitoring [e.g. authentication, badges, logs, etc.]).



Recommendations for finding #1

1. Review and become familiar with “shall” statements within the CJIS Security Policy to ensure requirements are being met within the agency.
1. Fully review returned spreadsheets, user guides, and/or other audit materials to ensure requested documentation fulfills all requirements.
1. When creating policies, they should be tailored to the agency’s processes & procedures regarding CJI. Avoid copying entire sections of the CJIS Security Policy as this doesn’t show what controls are in place.



CJIS Audit Findings (cont'd)

Inadequate Security Awareness Training

All agencies with access to CJIS must follow the training content & frequency requirements outlined in section 5.2.1 of the CJIS Security Policy. The top reasons security awareness training programs are inadequate are:

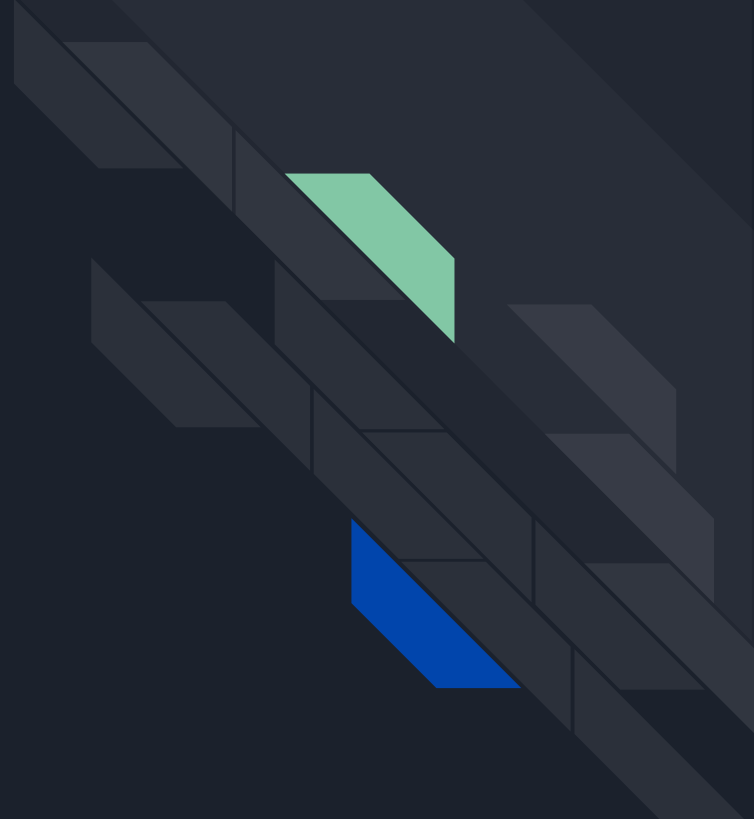
1. All applicable training levels & topics are not addressed with all appropriate personnel.
1. Training is not fully documented / not kept up to date.



Recommendations for finding #2

1. Training materials can be obtained from Utah BCI or purchased from KnowBe4.com & CJISonline.com. Agencies can also create their own training materials as long as all applicable topics are addressed.
1. The required topics that must be addressed as baseline security awareness training for each individual are dependent upon the level of access to CJI (non-user, non-access user, user, IT).
1. Documentation of training should be kept current and include names, level of training received, and the date of most recent training or training expiration.

FBI Audit Findings





FBI Audit Findings

1. Noncriminal Justice Agency: Ensure appropriate agreements are implemented and signed with each noncriminal justice agency.

Requirement: When the agency receives IT services from a noncriminal justice (government) agency, such as city or county IT, a management control agreement must be in place between these two entities.

CJIS Security Policy > 5.1.1.4 Interagency and Management Control Agreements

“The NCJA shall sign and execute a management control agreement (MCA) with the CJA, which stipulates management control of the criminal justice function remains solely with the CJA.”



FBI Audit Findings (cont'd)

2. Private Contractors: Ensure the CJIS Security Addendum is adequately documented, implemented, and signed with all private contractor personnel.

Requirement: The Security Addendum must be signed and maintained for all unescorted private contractor personnel performing criminal justice functions (incl. off-site media destruction, software vendors, IT services).

[CJIS Security Policy > 5.1.1.5 Private Contractor User Agreements and CJIS Security Addendum](#)

“All private contractors who perform criminal justice functions shall acknowledge, via signing of the CJIS Security Addendum Certification page, and abide by all aspects of the CJIS Security Addendum.”



FBI Audit Findings (cont'd)

3. Security Awareness Training: Ensure all security awareness training requirements of the CJIS Security Policy are documented and implemented.

Requirement: All applicable security awareness training topics must be addressed as baseline security awareness training for all personnel and training must be documented.

CJIS Security Policy > 5.2.3 Security Training Records

“Records of individual basic security awareness training and specific information system security training shall be documented, kept current, and maintained.”



FBI Audit Findings (cont'd)

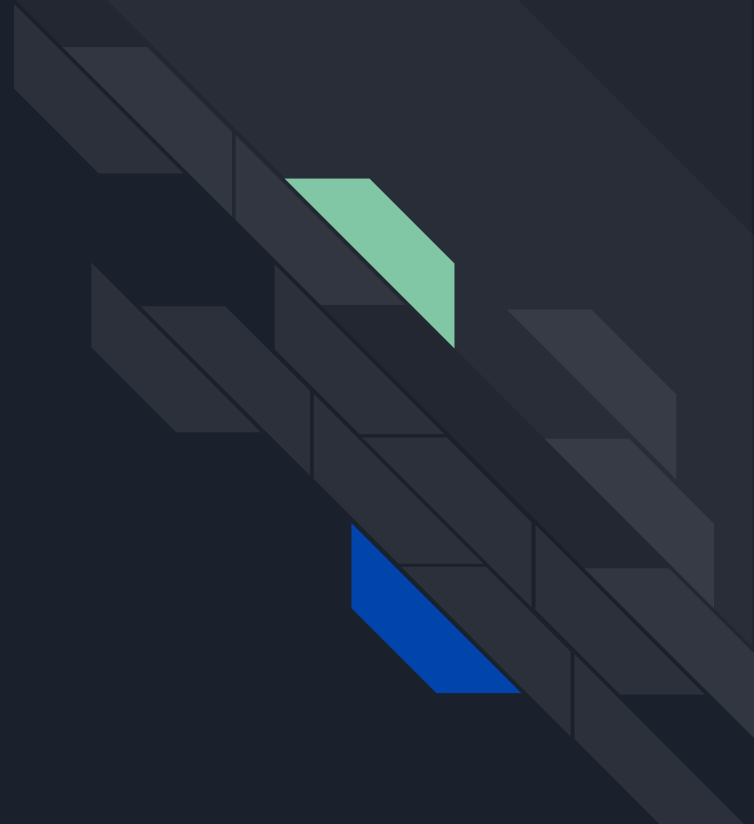
4. Advanced Authentication: Ensure advanced authentication is implemented for personnel who access or manage information systems containing CJJ from non-secure locations. These findings pertained to Spillman access in patrol vehicles.

Requirement: Currently, the FBI is allowing an alternative solution. A policy that indicates the laptops/Mobile Device Terminals(MDTs) will remain secured/locked in the vehicle's mounting stand, can be accepted instead.

CJIS Security Policy > 5.6.2.2.1 Advanced Authentication Policy and Rationale

“AA shall not be required for users requesting access to CJJ from within the perimeter of a physically secure location (Section 5.9), when the technical security controls have been met (Sections 5.5 and 5.10), or when the user has no ability to conduct transactional activities on state and national repositories, applications, or services (i.e. indirect access)”

CJIS Changes





CJIS Security Policy 5.9.1 - Changes

Core section changes

1. Media Protection 5.8 (MP)
2. Personnel Security 5.12 (PS)
3. Cloud Computing G.3 (CG)




5.8 Media Protection (MP)

Summary of Changes:

Modernize the CJIS Security Policy requirements for Media Policy & Procedures, Access, Marking, Storage, Transport, Sanitization and Use

- Complete section replacement
- All current requirements included but reformatted
- Several new requirements
 - MP-1c: Review and update policy and procedures...
 - MP-3 Media Marking
 - MP-7 Media Use



5.8 Media Protection (MP) - New Requirements

MP-1 Policy and Procedures

- Review and update Media Protection policies/procedures annually and following security incidents

MP-3 Media Marking

- Media must be appropriately marked to indicate its distribution limitations, handling caveats, and applicable security markings
 - Only applies to media that does not remain in physically secure locations or controlled areas

MP-7 Media Use

- Restrict use of media on systems that store, process, or transmit CJI
 - Port disabling, ACLs, GPO, MDM, other physical or administrative controls



Personnel Security 5.12 (PS)

Provide clarification of requirements:

- Personnel security requirements for cloud service providers: 5.12, 5.12.1
 - 5.12 Agency determines what is unescorted access to unencrypted CJI
 - Taking into consideration if those individuals have unescorted logical or physical access to any information system resulting in the ability, right, or privilege to view, modify, or make use of unencrypted CJI
 - 5.12.1 Based on type of service: IaaS, PaaS, SaaS - references G.3 Cloud Computing

G.3 Cloud Computing: Best Practices

- Additional language added to give guidance on personnel screening requirements specific to cloud environments based on the service in scope.
 - Cloud providers offer different levels of service, i.e.; Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). The way CJI is placed and accessed in the cloud determines if the personnel security requirements in Section 5.12 apply...



Upcoming 5.9.2 Changes

Three (3) new control families

- Awareness and Training (AT)
- Identification and Authentication (IA)
- System and Information Integrity (SI)

Two Administrative changes

- MP-2 - New example provided for non-digital media
- Appendix A - definition of “Non-digital media”



Frequently Asked Questions

- Why was I chosen as the LASO?
 - The LASO is typically the agency's technical representative and is chosen by the agency admin.
- Who is the agency's TAC / Admin?
 - Contact jarrelbeal@utah.gov for this information
- How does LASO Training differ from the training required for all personnel with access to CJI?
 - LASOs require enhanced training on the specific duties and responsibilities of those positions and the impact those positions have on the overall security of information systems.



FAQs (cont'd)

- Where can I access the CJIS Security Policy?
 - [CJIS Security Policy Resource Center](#)
- Who can I contact for policy or agreement samples?
 - Contact jarrelbeal@utah.gov



Contacts

Tyson Jarrett

CJIS Information Security Officer

385-255-0888

TJarrett@utah.gov

Jarrel Beal

CJIS Auditor

385-253-2420

JarrelBeal@utah.gov