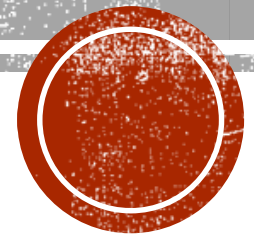
CJIS Audits

2022 TAC Conference



Agenda

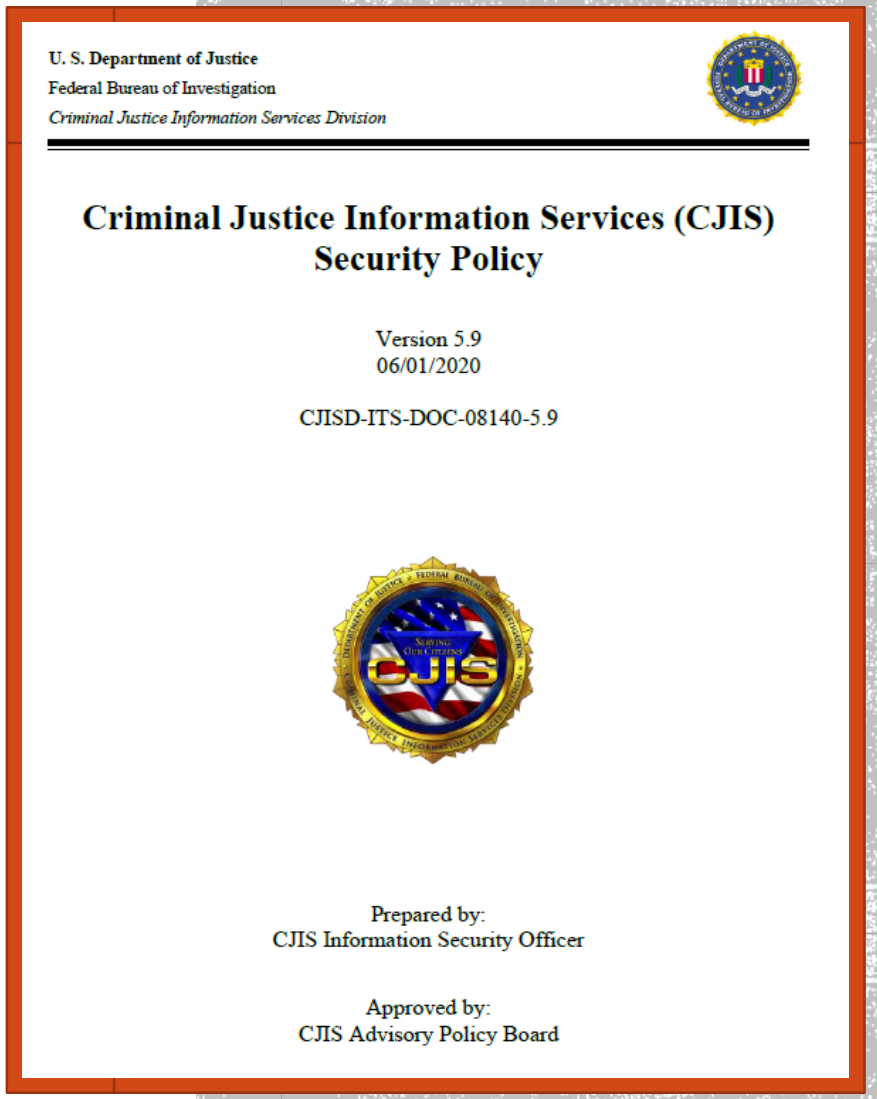
- Utah CJIS Structure
- CJIS Policy & Audit
- Audit Trends
- Helpful Resources
- Audit Process Update
- Q&A

Utah CJIS Structure

- The Criminal Justice Information Services repository is owned by the FBI.
- The FBI shares CJIS data with a CJIS Systems Agency (CSA) in each state. In Utah this is the Bureau of Criminal Identification within DPS.
- BCI houses this data, along with other data in the UCJIS Application.
- Each CSA has a CJIS Systems Officer (CSO) who is responsible for the administration of CJIS within Utah. This is Director Greg Willmore.
- Each CSA has an Information Security Officer (ISO) to serve as a point of contact to the FBI and to establish a security incident response & reporting procedure. This is Tyson Jarrett.
- Agencies who are granted rights to access this data for Law Enforcement purposes are Criminal Justice Agencies (CJA).
- Each CJA has a TAC to administer their CJIS environment and oversee compliance.
- Each CJA is required to have a Local Agency Security Officer (LASO) who is responsible for IT Security and supports policy compliance.

CJIS Security Policy

- This is the CJIS Security Policy (CSP) Version 5.9 (6/10/2020)
- The purpose of the CJIS Security Policy is to establish the minimum security requirements for the protection of CJI.
- 13 policy areas which agency must be aware of and uphold.



U. S. Department of Justice
Federal Bureau of Investigation
Criminal Justice Information Services Division

Criminal Justice Information Services (CJIS) Security Policy

Version 5.9
06/01/2020

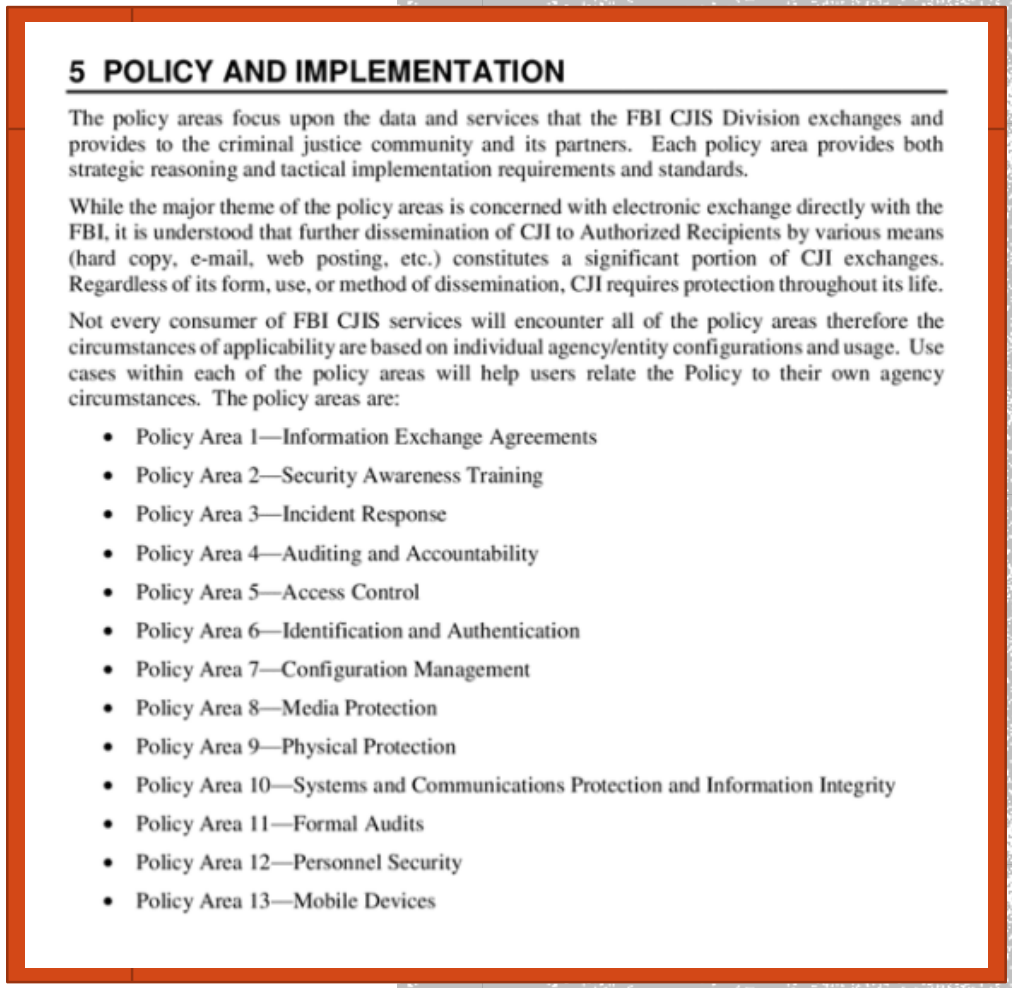
CJISD-ITS-DOC-08140-5.9

Prepared by:
CJIS Information Security Officer

Approved by:
CJIS Advisory Policy Board

Policy Areas

- Agencies can have a either: A comprehensive security policy **OR** separate policies that incorporate controls from the CJIS Security Policy.
- The policies should be documented and align with the policy areas of the CSP.
- Policies should be tailored to incorporate only the controls in place at the agency. (Specific to the agency's implementation)



5 POLICY AND IMPLEMENTATION

The policy areas focus upon the data and services that the FBI CJIS Division exchanges and provides to the criminal justice community and its partners. Each policy area provides both strategic reasoning and tactical implementation requirements and standards.

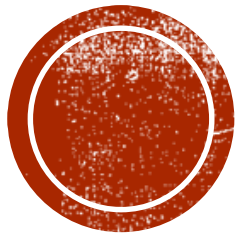
While the major theme of the policy areas is concerned with electronic exchange directly with the FBI, it is understood that further dissemination of CJI to Authorized Recipients by various means (hard copy, e-mail, web posting, etc.) constitutes a significant portion of CJI exchanges. Regardless of its form, use, or method of dissemination, CJI requires protection throughout its life.

Not every consumer of FBI CJIS services will encounter all of the policy areas therefore the circumstances of applicability are based on individual agency/entity configurations and usage. Use cases within each of the policy areas will help users relate the Policy to their own agency circumstances. The policy areas are:

- Policy Area 1—Information Exchange Agreements
- Policy Area 2—Security Awareness Training
- Policy Area 3—Incident Response
- Policy Area 4—Auditing and Accountability
- Policy Area 5—Access Control
- Policy Area 6—Identification and Authentication
- Policy Area 7—Configuration Management
- Policy Area 8—Media Protection
- Policy Area 9—Physical Protection
- Policy Area 10—Systems and Communications Protection and Information Integrity
- Policy Area 11—Formal Audits
- Policy Area 12—Personnel Security
- Policy Area 13—Mobile Devices

CJIS Audit

- Every agency will be audited at least every 3 years.
- Purpose of the audit is to ensure compliance with the CJIS Security Policy.
- When it is time for the agency's audit, the TAC will be contacted.
- TACs are responsible for ensuring that policies and agreements are in place and documented.
- The TAC & LASO should work together to complete the audit and support CJIS compliance.



Audit Trends

Common Audit Findings

- **Policies**
  - Not documented or haven't been implemented
  - Haven't been reviewed/revised recently
  - Copied from the CJIS Security Policy
  - Not tailored to agency's implementation

- **Other Challenges**
  - TAC/LASO unfamiliar with CJIS Security Policy requirements
  - Inadequate Security Awareness Training
    - Missing topics
    - Appropriate levels/topics not being addressed
    - Not thoroughly documented
  - Incident Response plan
    - Not fully developed
    - CJIS ISO should be contacted vs. FBI

Recommendations

- Review CJIS Security Policy section 5 to ensure familiarity with agency's requirements.
- Regularly review agency policies to ensure they're up to date and "audit-ready"
- Collaborate with LASO and ensure they are familiar with CSP and technical requirements.
  - Supplemental LASO Training will be provided by DPS in the future
- Look into available forums for collaboration and other tips. JusticeConnect is a great option to consider.

Helpful Resources

Services

- Special Interest Groups (SIG)
- Virtual Command Center (VCC)
- National Data Exchange (N-DEx)
- Joint Automated Booking System (JABS)
- INTELINK
- Regional Information Sharing Systems Network (RISS)
- National Gang Intelligence Center (NGIC)
- eGuardian
- FBI Virtual Academy (VA)
- Internet Crime Complaint Center (IC3)
- Cyber Investigation Certification Program (CICP)
- Violent Criminal Apprehension Program (ViCAP)
- Plus many more . . .

Contact Us

LEEP Support Center
888-334-4536, toll-free domestic calls
225-334-4536, international calls
711, Telecommunication Relay Service
helpdesk@leo.gov

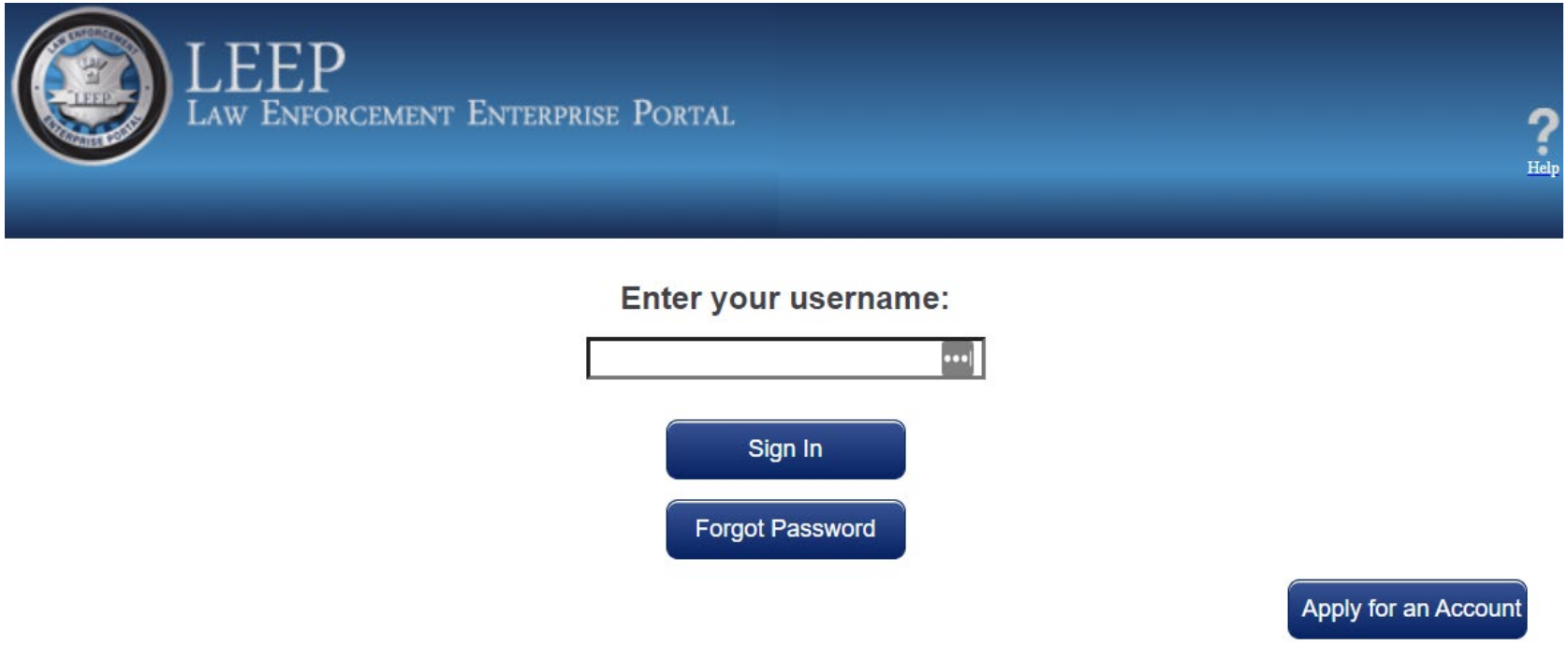
U.S. Department of Justice
Federal Bureau of Investigation
Criminal Justice Information Services Division

Law Enforcement Enterprise Portal

Secure Access to the Services You Rely On.

Resources Available
Users can strengthen case development with the investigative tools available, collaborate with internal and external agencies, and securely share sensitive documents. Examples of resources available include:

- **40+ service providers**
- **Nationwide criminal justice records**
- **Global cyber-complaint data**
- **Counterterrorism threat tracking**
- **Intelligence centers**
- **Gang Information**
- **Information sharing networks**
- **File Sharing**
- **And much more!**

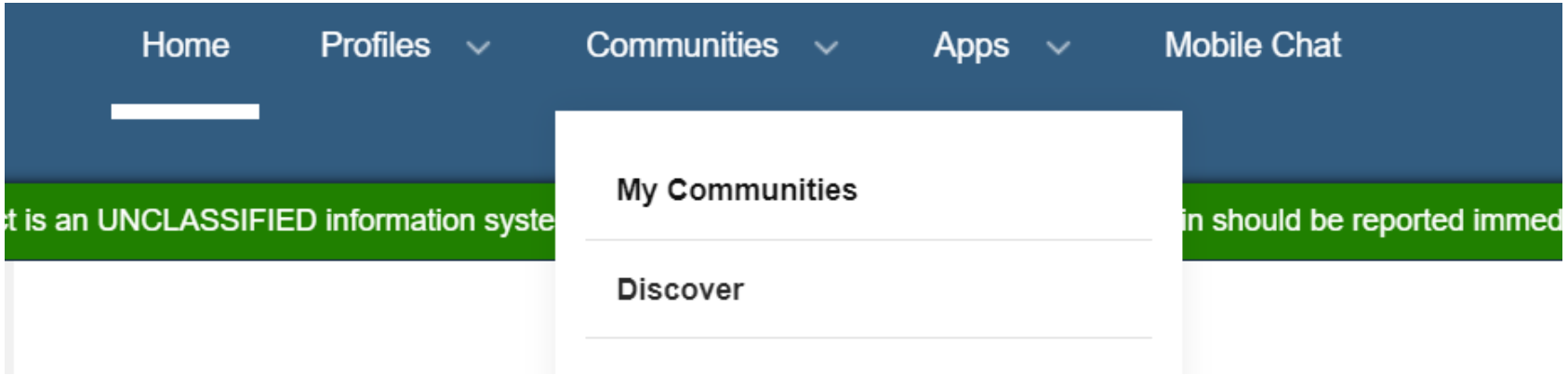


Law Enforcement Enterprise Portal

The FBI has established the "Law Enforcement Enterprise Portal" (LEEP). A secure platform designed to support collaboration and coordination. Available to personnel affiliated with the criminal justice system.

Through LEEP you can gain access to JusticeConnect. A tool to share & store information to enhance collaboration among CJAs, emergency management & intelligence experts.

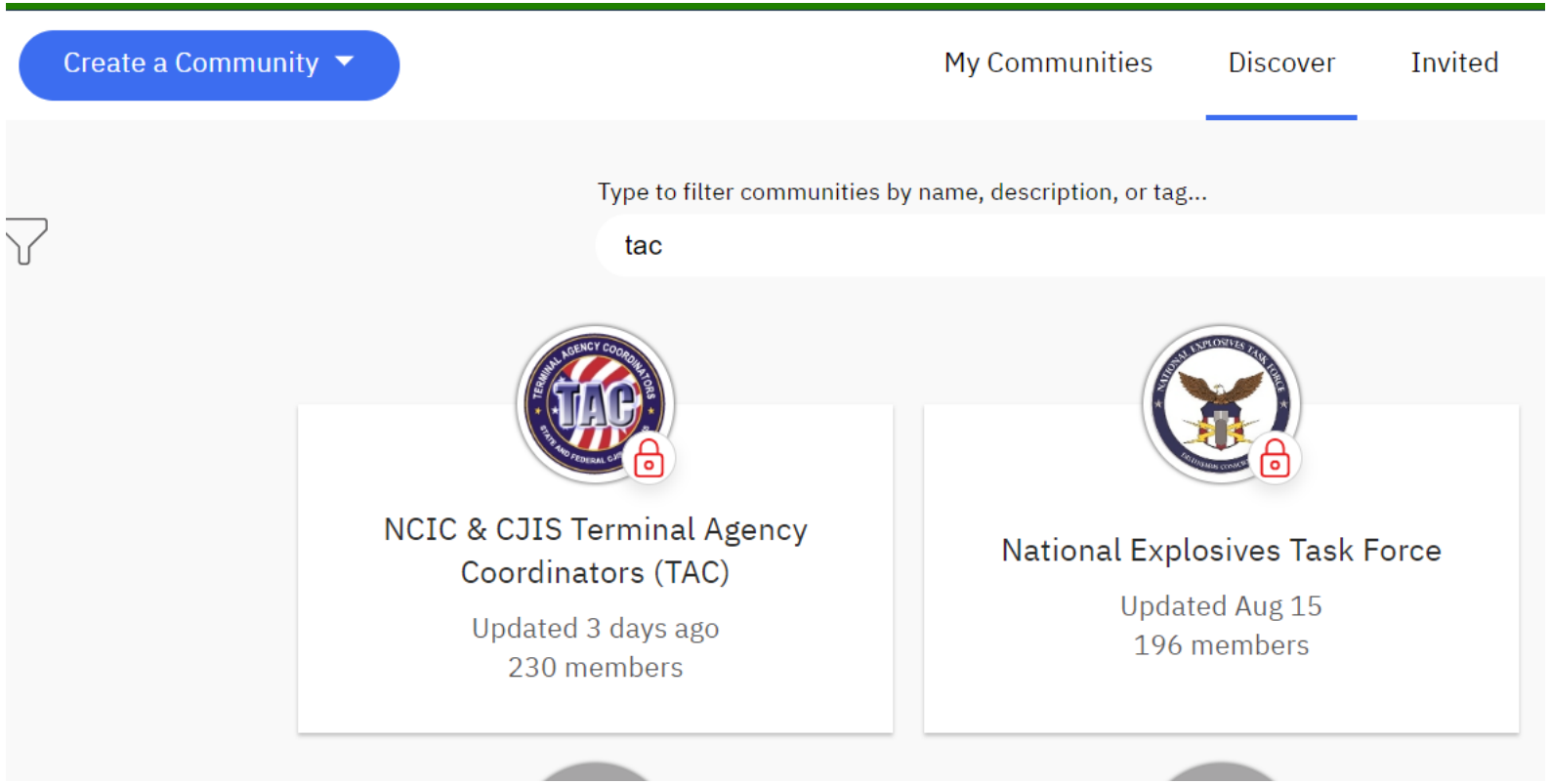
1. Select JusticeConnect within the top ribbon



2. Then under the "Communities" drop down look for "Discover"

JusticeConnect

"JusticeConnect is an innovative, new online collaboration service accessible via LEEP. Through online forums and blogs, partners can communicate with experts, share information and ideas, and receive feedback with criminal investigations."



Once here, you can either create a new community or search for one you are interested in.

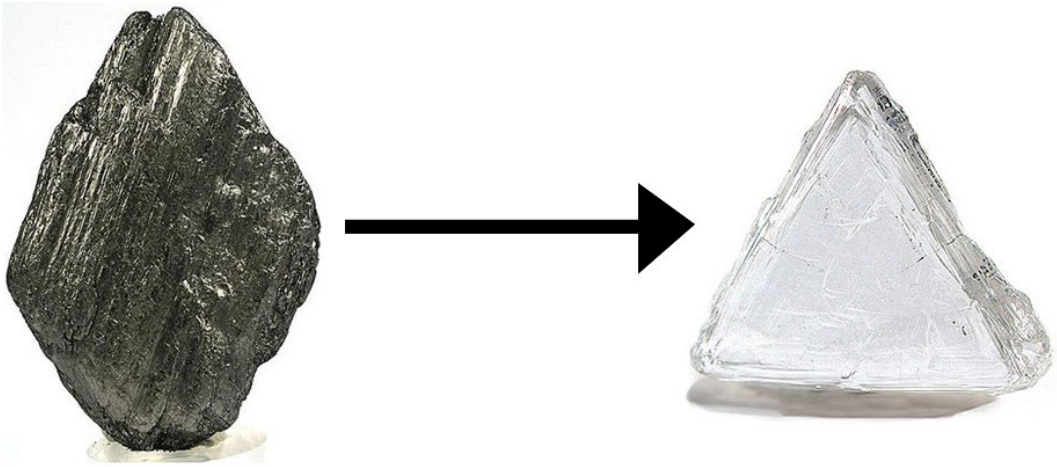
JusticeConnect

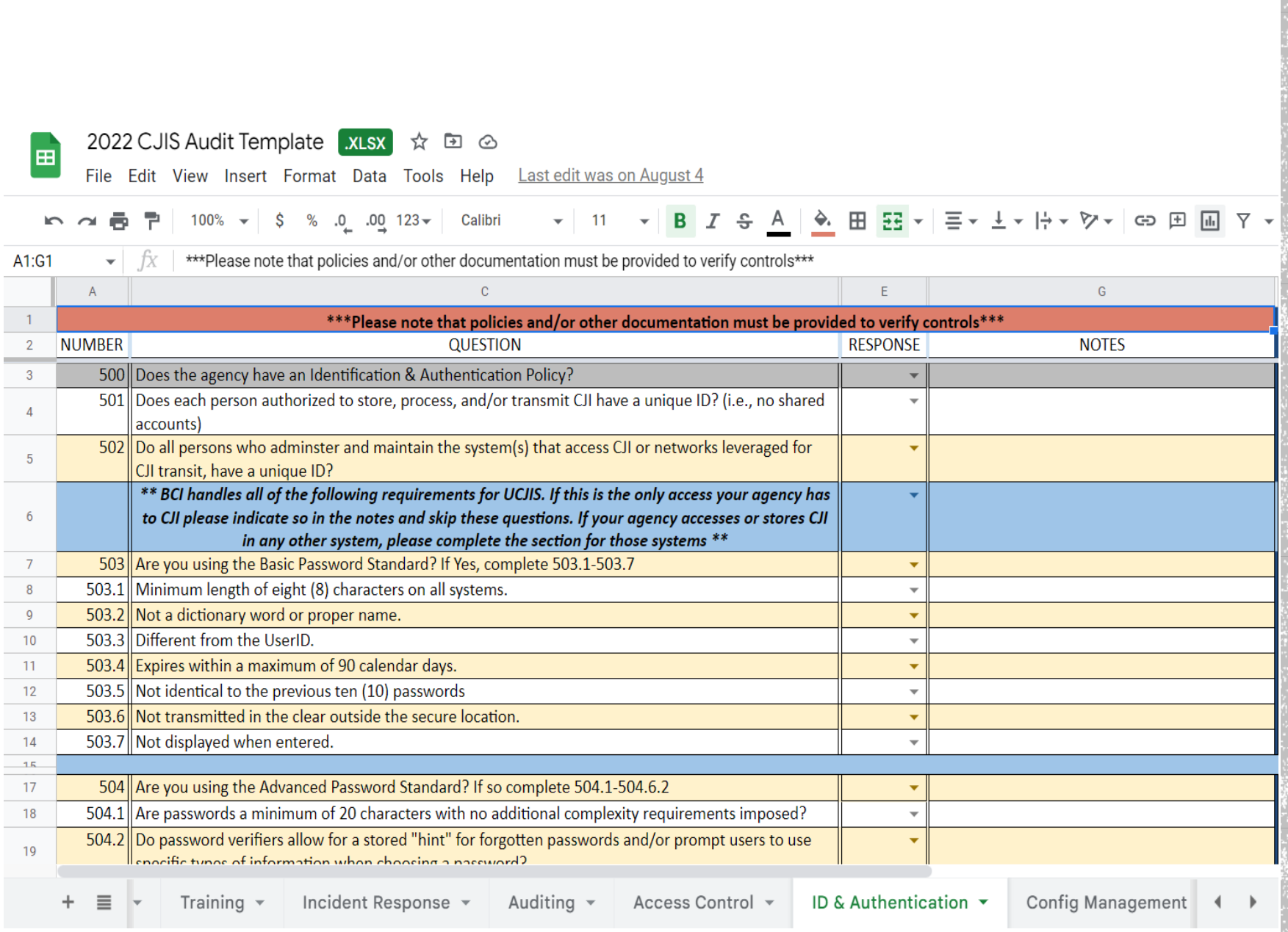
Finding a community that works for you

Audit Process Update

Audit Transition

- The process in which we are conducting the remaining CJIS audits this cycle has been updated.
- The existing audit process (V.0) has received substantial and consistent feedback that needed to be addressed.
- The new process (V.1) was created to address the feedback and inefficiencies of the previous process.





V.0 / The Spreadsheet

Challenges

- Too confusing for agencies
- Scope is too broad
- Doesn't focus on risks
- Unnecessary / incorrect documentation submitted

Addressing the Feedback

Prior Issues		Addressed?	Key Points

1	Confusing / Not Intuitive	✓	• Audit meeting with TAC
			  ○ Discuss agency infrastructure and applicability
			  ○ Guide through process

2	Burdensome / Time Consuming	✓	• No spreadsheet • Reduced scope • Documentation requests are minimized

3	Broad Focus	✓	• Risk based scope:
			  ○ Account Management
			  ○ Physical Security
			  ○ Encryption

4	Inconsistent Documentation	✓	• User guides are provided to give more clarity ○ Includes checklist to ensure documentation meets all requirements

Pre-Audit Discussion Questions (sample)

4. Which systems/applications does your agency use to view, access, store or transmit CJI? (e.g. UCJIS, Spillman, Cloud Storage Provider, Email client)

5. Does a separate entity or agency host your CAD/RMS (Fatpot / Spillman) instance?
    a. If yes, who is the administering agency?

6. Do you administer a CAD/RMS instance to other agencies?
    a. If yes, which agencies?

7. Does your agency have documented policies in place that align with the policy areas outlined in the CJIS Security Policy?
    a. Who owns and/or maintains these policies?
    b. Are the policies tailored to the controls in place at your agency or are they copied from the CJIS Security Policy?

8. Indicate if CJI is:
    a. Printed? (If yes):
        i. What is printed?
        ii. Is it stored or immediately destroyed/put in a shred bin?

    b. Transmitted outside the boundary of the physically secure location? (e.g. When leaving the local area network or building / being sent via email)
        i. Method of transmission
        ii. Is the method FIPS 140-2 certified?

    c. Stored (digitally) outside the boundary of the physically secure location? (cloud storage)
        i. Is the data encrypted?

V.1 / The Questionnaire

Benefits

- **TACs are lead through audit**
- **Focused audit scope based on risk**
- **Minimized documentation requests**

Utah CJIS Audit Agency Guide

CJIS Security Policy Area 5: Access Control

5.5.1 - Account Management

The agency shall manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The agency shall validate information system accounts at least annually and shall document the validation process. The agency shall identify authorized users of the information system and specify access rights/privileges.

Applicability:

This requirement applies to:

1. CJIS systems (i.e. UCJIS, CAD & RMS systems: Spillman, Tyler Tech, etc.)

Documentation Checklist:

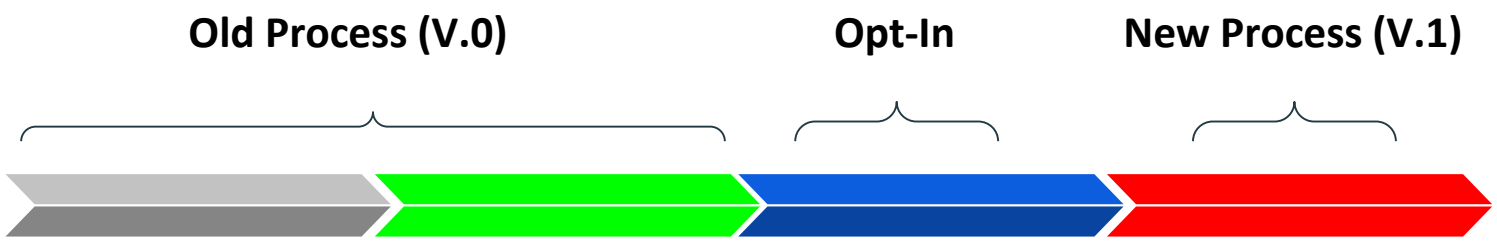
- ☐ **Identification of current individuals with CJIS access:**
  - ☐ List of personnel with CJIS access including:
    - ☐ Name / User-ID(s)
    - ☐ CJIS System(s)
    - ☐ Access level (user, non-access user, etc.)
    - ☐ Date access was granted (if within last 3 years)
- ☐ **Access Control policy incorporating:**
  - ☐ Agency's requirement to validate CJIS system accounts at least annually
  - ☐ Description of process to establish least privilege access (valid need-to-know/need-to-share) that is determined by assigned official duties
  - ☐ Description of process on managing changes to CJIS access when user is terminated or transferred
- ☐ **Information System Account Validations:**
  - ☐ Proof of most recent annual account review for *each* CJIS system

New audit format / User Guides

Benefits

- **Leads to correct documentation being sent initially**
- **Outlines exactly what is needed**
- **Checklist to ensure all requirements are incorporated**

Who this applies to



Audit Submitted

Agency was sent the audit spreadsheet and submitted it back to me. Still **pending review / completion** .

Audit Complete

Spreadsheet and all supporting documents were submitted and **agency was notified** that audit was complete for this cycle.

Audit Started

Spreadsheet was sent to agency but **response has not been submitted.**

Audit Not Started

Spreadsheet **has not been sent** to agency.

Next Steps

- TACs should coordinate with LASOs to ensure familiarity with CJIS Security Policy requirements and that Security Addendums are in place.
- V.1 of the audit process is being tested and finalized
- Roll-out expected to begin in November with the "Opt-In" group
- All audits moving forward will be using the V.1 format (unless another update occurs)

QUESTIONS?

- CJIS ISO
  - Tyson Jarrett
  - Tjarrett@utah.gov
  - 385-255-0888
- CJIS Auditor
  - Jarrel Beal
  - Jarrelbeal@utah.gov
  - 385-253-2420