CJIS IT AUDITS

Lani Dick and Roxanne Scoggan

ISO Team

2021 TAC Conference

WHY AN IT AUDIT TRAINING?

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 the ultimate voice for CJIS within Utah. In Utah this is Captain Greg Willmore.
- One of the roles of the CSO is to appoint a CJIS Information Security Officer (ISO) to manage the IT Security Program for CJIS sharing within Utah.
- Agencies who are granted rights to access this data for Law Enforcement purposes are Criminal Justice Agencies (CJA).
- Each CJA has a TAC (You) to administer their CJIS environment and oversee compliance.
- And also a Local Agency Security Officer (LASO) who is responsible for the IT Security within the CJA.
- The LASO and TAC are responsible for completing an IT Audit once every 3 years.

TRANSITION & INTRODUCTIONS

- Historically the role of the CJIS ISO, or Information Security Officer, was held by DTS, most recently Garry Gregson for a number of years.
- With Garry accepting a new position in December, the decision was made to transition the role to a DPS position, as DPS owns the data, and now has an Agency Information Security Officer.
- The DPS ISO will still partner with the DTS Security Analyst, as well as BCI, to transition the CJIS ISO Program.

- New CJIS ISO:
  - Lani Dick
  - lani@utah.gov
  - 801-386-6964
- DTS Security Partner
  - Roxanne Scoggan
  - rscoggan@utah.gov
  - 385-254-1091
  - Working to hire additional personnel to assist in the upcoming IT Audit Cycle.

SO, WHY AN IT AUDIT TRAINING?

- Because we are going through a transition period! We want to introduce ourselves to you and explain how we plan to move forward with the IT Audit program.
- Just as we are working to collaborate further with BCI, it's important that TACs and LASOs collaborate more on the IT Audits. Both have a role and a responsibility.
- We also want to acknowledge that we are both very new to the CJIS program, so we are learning with you. We are open to suggestions and feedback and want to build a program that works for you as well as it does for us.
- But this also means we may take a little longer to provide responses as we work to research, collaborate and consult with the FBI to ensure we are making correct decisions.

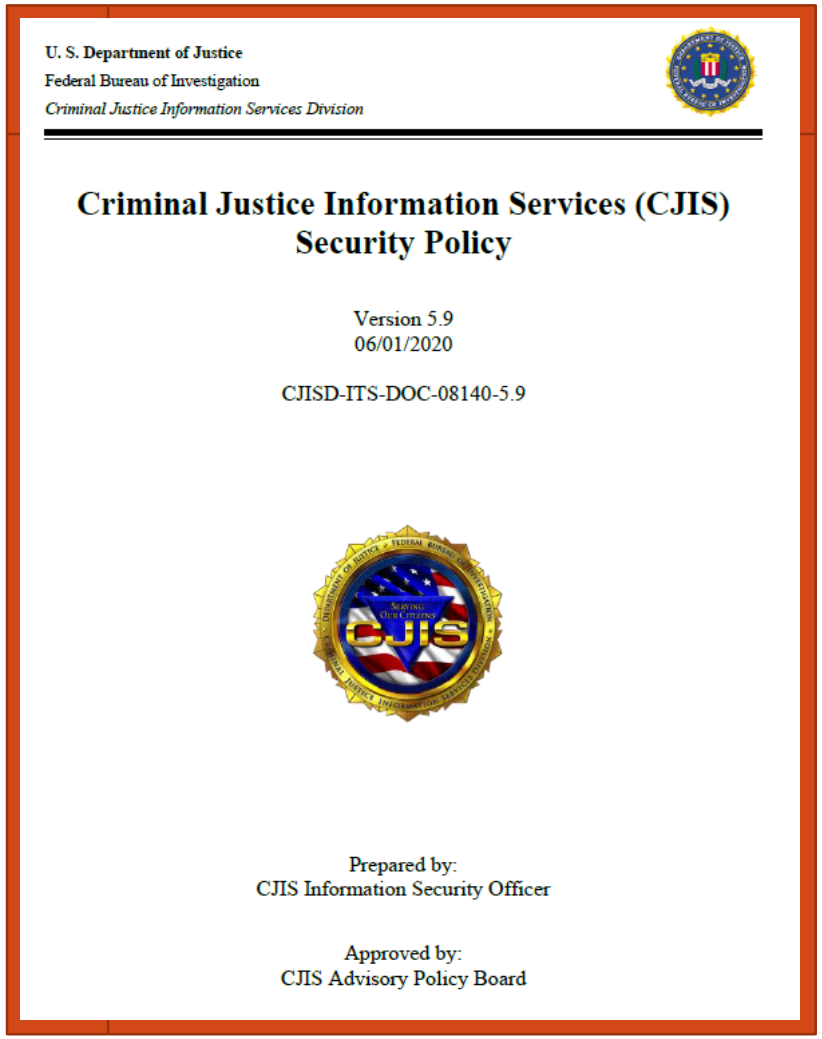
SO, LET'S GET STARTED!

There ***IS*** a CJIS Security Policy!
CSP Version 5.9 (6/10/2020)

https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center

This is an excellent resource and a good way to familiarize yourself with the compliance requirements for your IT Audit.

But, remember that BCI is the owner and steward of CJIS in Utah and makes the final decisions on how policy is applied. If you have questions, please reach out!



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

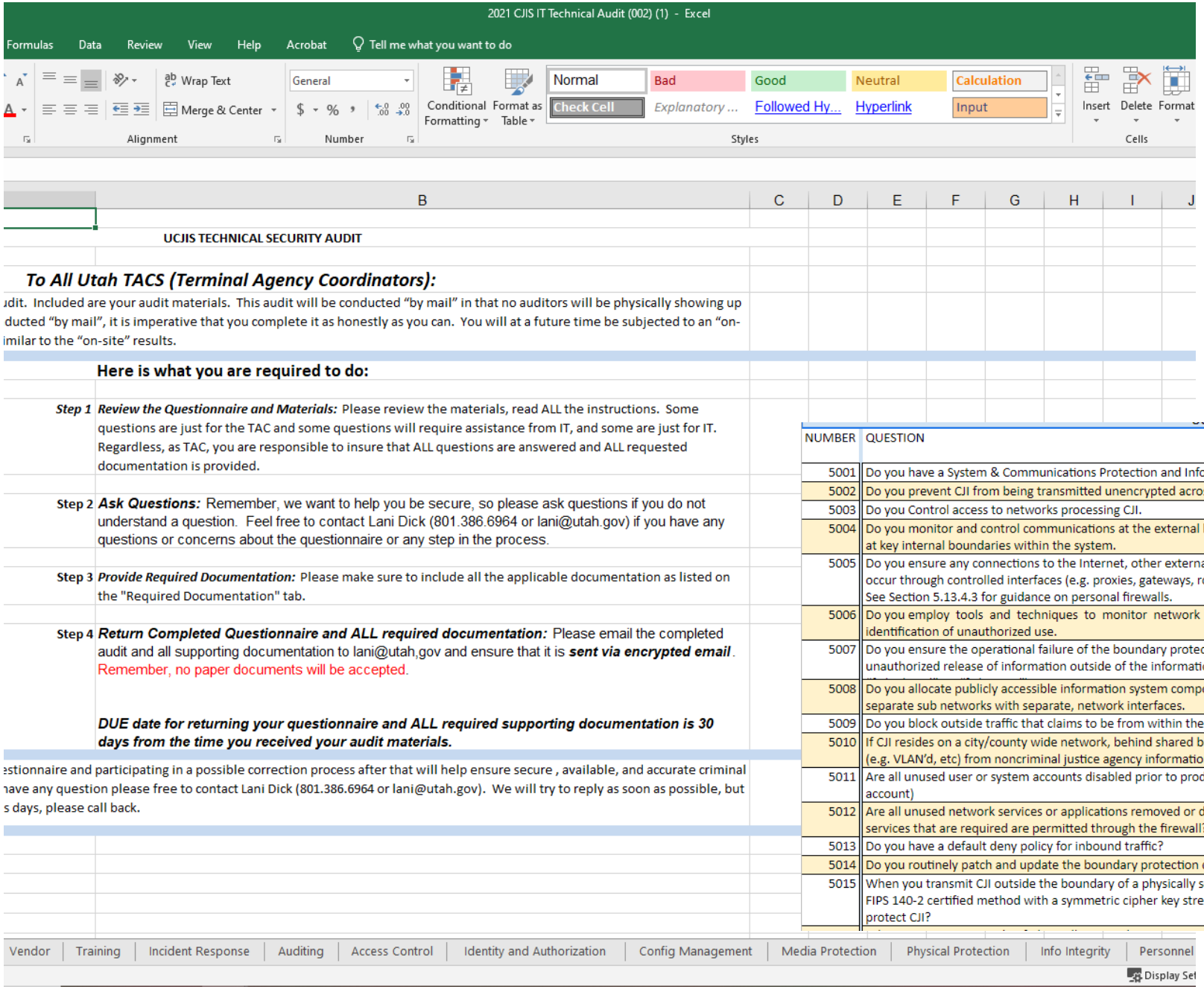
CJISD-ITS-DOC-08140-5.9

Prepared by:
CJIS Information Security Officer

Approved by:
CJIS Advisory Policy Board

PRIOR IT AUDIT

Some of you may recognize the prior Excel Spreadsheet version of the IT Audit for Utah. This is one of the most significant changes we will be making in the upcoming audit cycle as we move away from this format.



2021 CJIS IT Technical Audit (002) (1) - Excel

Formulas Data Review View Help Acrobat Tell me what you want to do

Wrap Text Merge & Center Alignment

General Number

Conditional Formatting Format as Table

Normal Bad Good Neutral Calculation Check Cell Explanatory ... Followed Hy... Hyperlink Input Styles

Insert Delete Format Cells

UCJIS TECHNICAL SECURITY AUDIT

To All Utah TACS (Terminal Agency Coordinators):

dit. Included are your audit materials. This audit will be conducted "by mail" in that no auditors will be physically showing up ducted "by mail", it is imperative that you complete it as honestly as you can. You will at a future time be subjected to an "on- imilar to the "on-site" results.

Here is what you are required to do:

Step 1 ***Review the Questionnaire and Materials:*** Please review the materials, read ALL the instructions. Some questions are just for the TAC and some questions will require assistance from IT, and some are just for IT. Regardless, as TAC, you are responsible to insure that ALL questions are answered and ALL requested documentation is provided.

Step 2 ***Ask Questions:*** Remember, we want to help you be secure, so please ask questions if you do not understand a question. Feel free to contact Lani Dick (801.386.6964 or lani@utah.gov) if you have any questions or concerns about the questionnaire or any step in the process.

Step 3 ***Provide Required Documentation:*** Please make sure to include all the applicable documentation as listed on the "Required Documentation" tab.

Step 4 ***Return Completed Questionnaire and ALL required documentation:*** Please email the completed audit and all supporting documentation to lani@utah,gov and ensure that it is ***sent via encrypted email***. Remember, no paper documents will be accepted.

DUE date for returning your questionnaire and ALL required supporting documentation is 30 days from the time you received your audit materials.

estionnaire and participating in a possible correction process after that will help ensure secure , available, and accurate criminal ave any question please free to contact Lani Dick (801.386.6964 or lani@utah.gov). We will try to reply as soon as possible, but s days, please call back.

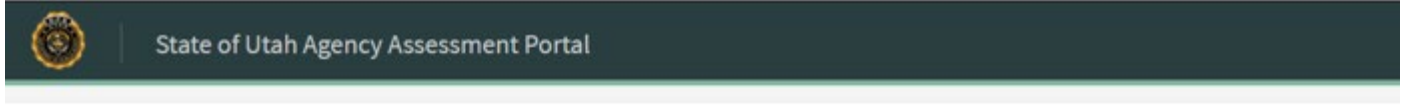
NUMBER	QUESTION
5001	Do you have a System & Communications Protection and Information Integrity Policy?
5002	Do you prevent CJI from being transmitted unencrypted across the public network?
5003	Do you Control access to networks processing CJI.
5004	Do you monitor and control communications at the external boundary of the information system and at key internal boundaries within the system.
5005	Do you ensure any connections to the Internet, other external networks, or information systems occur through controlled interfaces (e.g. proxies, gateways, routers, firewalls, encrypted tunnels). See Section 5.13.4.3 for guidance on personal firewalls.
5006	Do you employ tools and techniques to monitor network events, detect attacks, and provide identification of unauthorized use.
5007	Do you ensure the operational failure of the boundary protection mechanisms do not result in any unauthorized release of information outside of the information system boundary (i.e. the device
5008	Do you allocate publicly accessible information system components (e.g. public Web servers) to separate sub networks with separate, network interfaces.
5009	Do you block outside traffic that claims to be from within the agency?
5010	If CJI resides on a city/county wide network, behind shared boundary protection, is the CJI separated (e.g. VLAN'd, etc) from noncriminal justice agency information systems?
5011	Are all unused user or system accounts disabled prior to productions release? (i.e., vendor, admin account)
5012	Are all unused network services or applications removed or disabled to ensure that only network services that are required are permitted through the firewall?
5013	Do you have a default deny policy for inbound traffic?
5014	Do you routinely patch and update the boundary protection device/firewall?
5015	When you transmit CJI outside the boundary of a physically secure location is it encrypted using a FIPS 140-2 certified method with a symmetric cipher key strength of at least 128 bit strength to protect CJI?

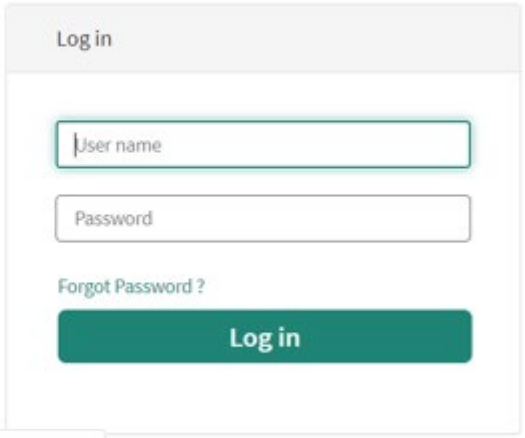
Vendor | Training | Incident Response | Auditing | Access Control | Identity and Authorization | Config Management | Media Protection | Physical Protection | Info Integrity | Personnel

Display Se

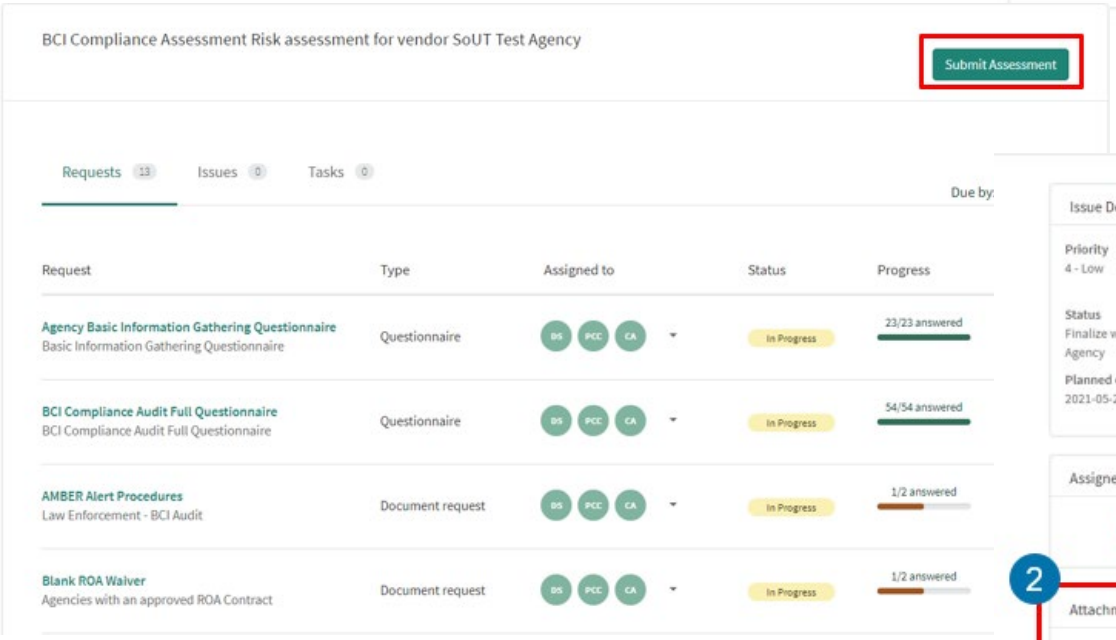
NEW IT AUDIT

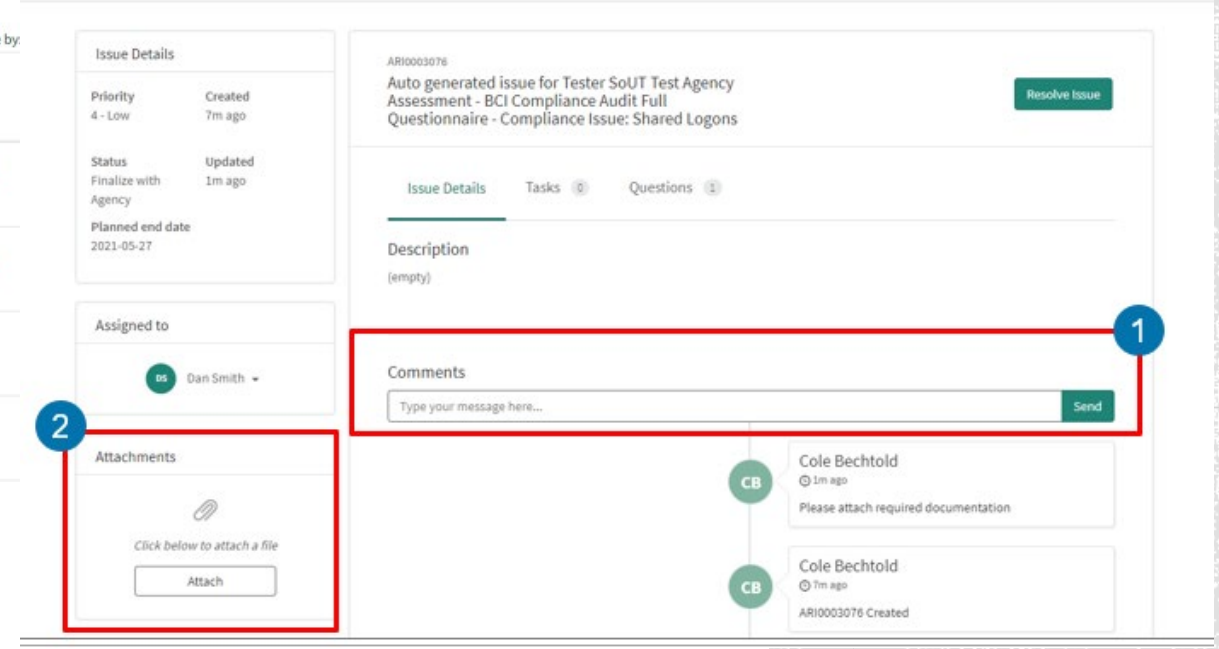
[dpsutah.servicenowservices.com/SVDP]





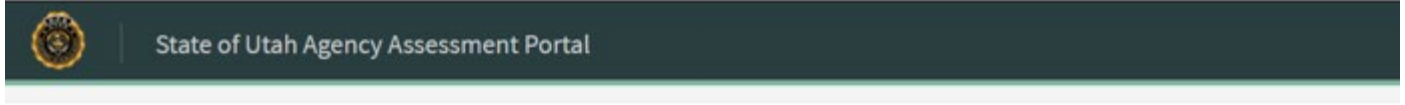
BCI has purchased a Service Now software to use for all CJIS Audits. The State of Utah Agency Assessment Portal will alert you to audits and deadlines and allow you to complete your questionnaires and upload documentation.

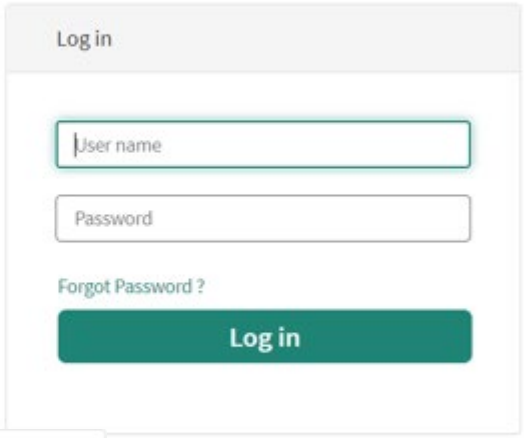


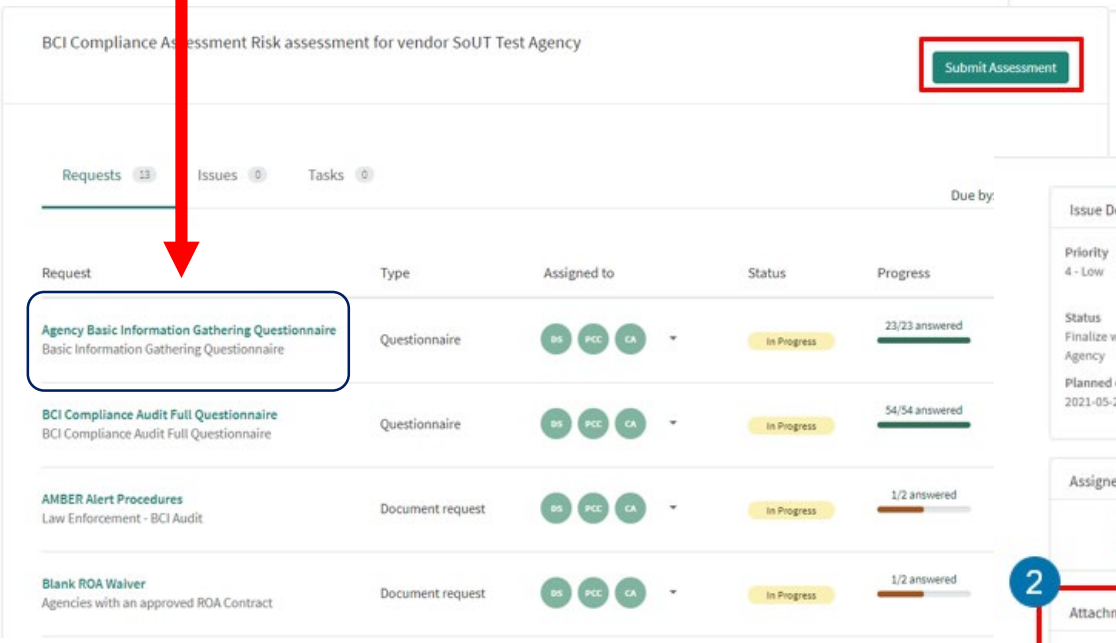


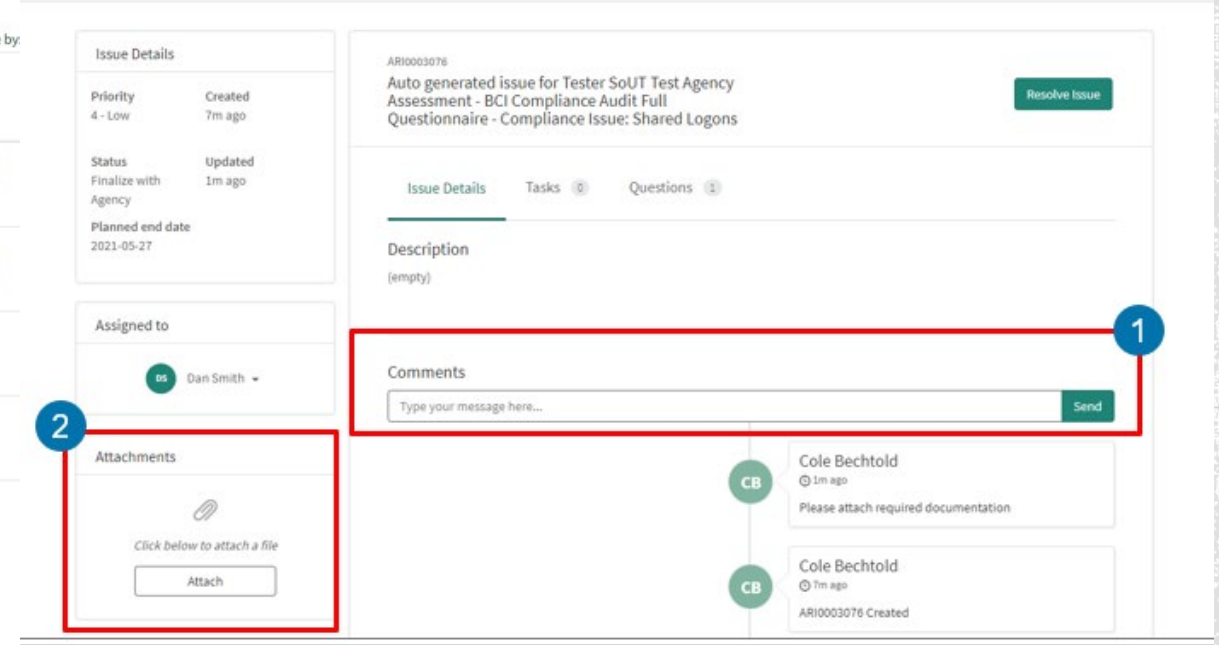
TWO QUESTIONNAIRES

[dpsutah.servicenowservices.com/SVDP]







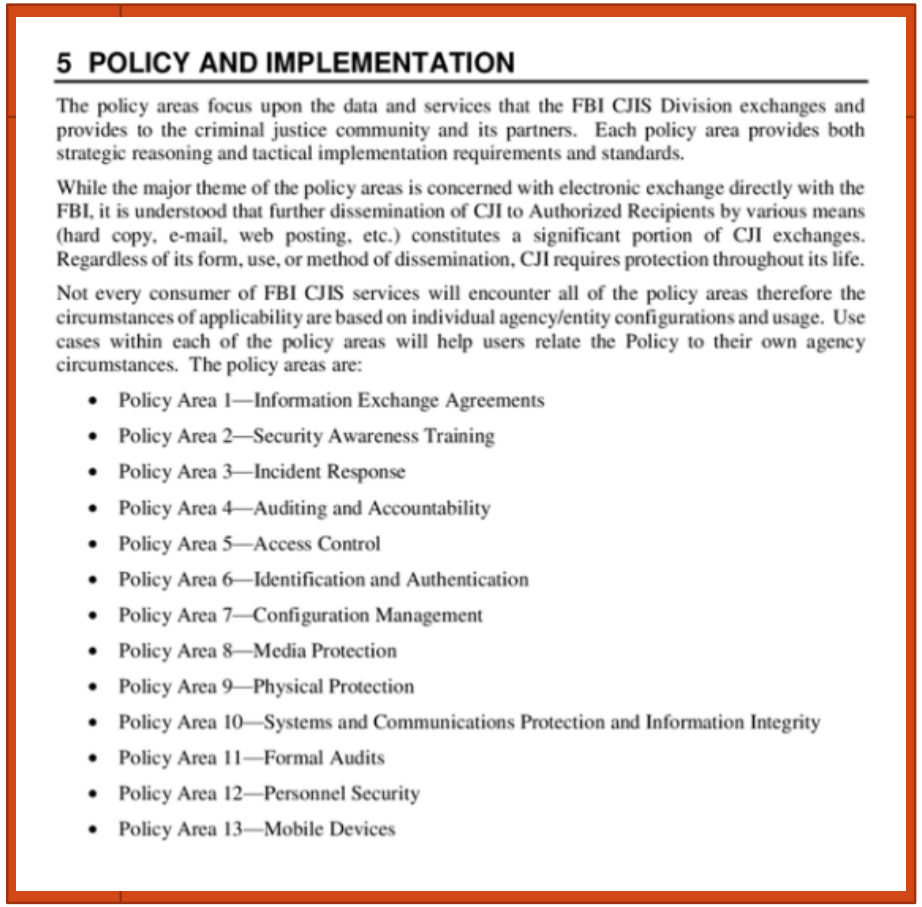


IT Audit broken into two sections:

1) Agency Basic Information Gathering Questionnaire
2) CJIS IT Audit
    1) IT Questions
    2) Document Verifications

CONTENT OF THE IT AUDIT

- Aligns with standard Information Security Practices
- Broken down into 13 primary policy areas
- Many are IT specific (LASO), but many should be familiar to you as a TAC – such as Security Awareness Training, Personnel Security, Information Exchange Agreements and Incident Response



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.

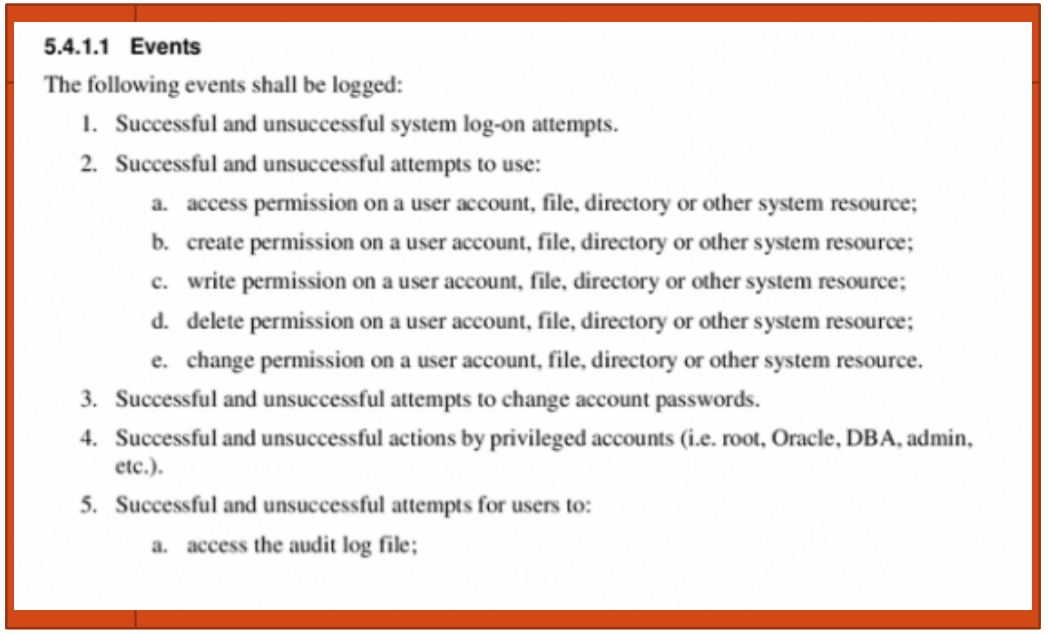
While the major theme of the policy areas is concerned with electronic exchange directly with the FBI, it is understood that further dissemination of CJI to Authorized Recipients by various means (hard copy, e-mail, web posting, etc.) constitutes a significant portion of CJI exchanges. Regardless of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

CONTENT OF THE IT AUDIT

- Each of the 13 sections contain a number of "shall" statements which are the basis of the IT Audit
- These "Shall" statements must be acknowledged and verified during the IT Audit.
- The example here is the requirement for system logging which may be met by providing settings from your logging tool, sample logs for review, or active policies.



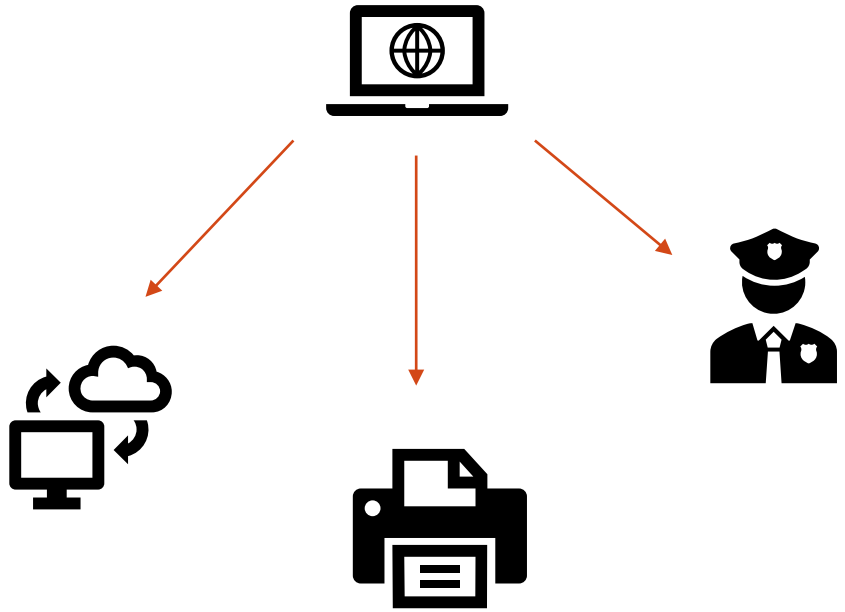
5.4.1.1 Events

The following events shall be logged:

1. Successful and unsuccessful system log-on attempts.
2. Successful and unsuccessful attempts to use:
    a. access permission on a user account, file, directory or other system resource;
    b. create permission on a user account, file, directory or other system resource;
    c. write permission on a user account, file, directory or other system resource;
    d. delete permission on a user account, file, directory or other system resource;
    e. change permission on a user account, file, directory or other system resource.
3. Successful and unsuccessful attempts to change account passwords.
4. Successful and unsuccessful actions by privileged accounts (i.e. root, Oracle, DBA, admin, etc.).
5. Successful and unsuccessful attempts for users to:
    a. access the audit log file;

CONTENT OF THE IT AUDIT

- Audits are applicable to your entire CJIS environment – from the initial access of CJIS to anywhere else it is processed, transmitted or stored.
- Consideration must be given to 3rd party partners as well – Examples are CAD and RMS systems. Agreements must be in place for vendor access to data and responsibilities for CJIS compliance.
- Remember CJA requirements differ from NCJA!



2021 AUDIT CYCLE

- Every agency will be audited over the next three years, until the FBI returns.
- Your agency (TAC/LASO) will be contacted when it is time for your audit.
- The ISO Team will work with your agency to ensure all required documentation is obtained.
- Once complete, your agency will be notified about any areas of non-compliance which must be addressed. A POAM will be expected to monitor progress.
- This audit cycle will be comprehensive to address all areas of compliance within all agencies.
- The goal is to reach a sustainable level of compliance so that the next audit cycle can allow us to being "Audit sampling", similar to how the FBI completes their triennial audits.

AREAS OF CONCERN

AGREEMENTS

ON-CJA, your agreement

oblems

Finding from 2021 Audit and in process

Agreement)

Partners

- *Unescorted access to unencrypted data*

- Templates can be found in the CJIS Security Policy
  - Or may be included in other agreements (MOU, etc)

ENCRYPTION

- CJIS transmitted or accessed outside physically secure location
  - Encryption must be at least symmetric 128-bit
  - Must be FIPS 140-2 CERTIFIED

- CJIS At Rest
  - May be encrypted as above **– OR --**
  - Encryption must be at least symmetric 256-bit
  - Must be FIPS 197 (AES) Certified

- Public Key Encryption (Asymmetric) or Hybrid Models
  - Permitted with additional controls in place

https://www.nist.gov/standardsgov/compliance-faqs-federal-information-processing-standards-fips

Symmetric Encryption
One Key Session

Asymmetric Encryption
Two Key Session

Public Key

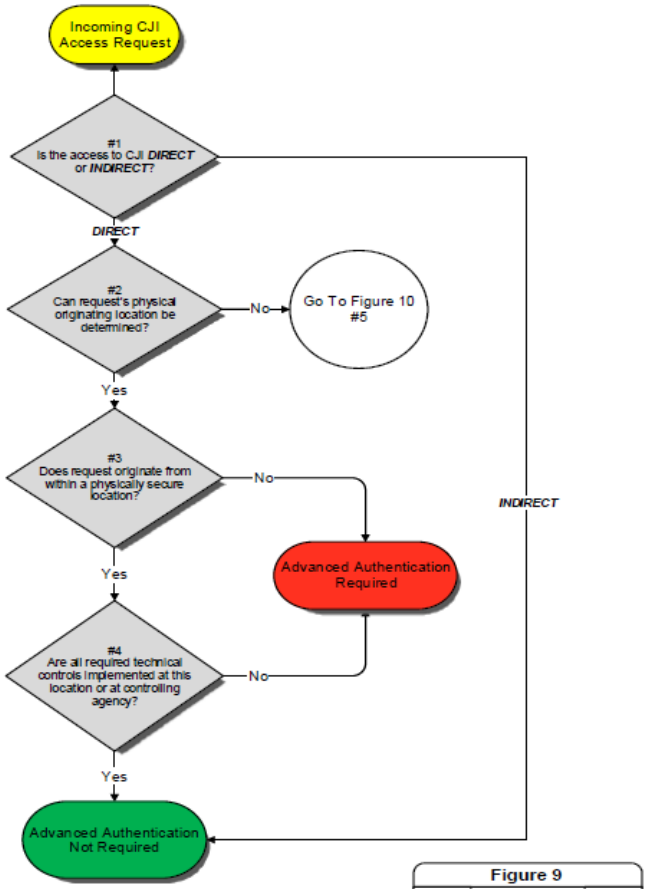
Private Key

ADVANCED AUTHENTICATION

- Advanced Authentication is different than Advanced Password Standards.
  - (MFA/2FA)

- When should AA be used?
  - Dependent on physical, personnel and technical security controls
  - Direct or Indirect Access
  - Dependent on system (UCJIS)
  - AA Section 5.6 of CJIS Security Policy. Figure 8 includes Use Cases and Figures 9 & 10 include Decision Trees.
  - 6.0 Modernization!!

Figure 9 – Authentication Decision for Known Location



POLICIES

- Anticipate findings for policy in most audits
- Internal Audits and FBI Report
  - Practices typically in place, but must be documented.
- Policies must be in place and known to users!

MOBILE DEVICES

- Mobile Devices are those that do not support a full OS, so does NOT apply to laptops. This is smart phones, (most) tablets, etc.
- Consideration for mobile devices also involves the question of BYOD devices which have additional controls.
- Where technical controls are not feasible, an agency may implement policy prohibiting the access of CJIS via mobile devices to reduce scope.
- MDM solutions – We only require that it meet the CSP requirements.

- Similar: Wireless

NUMBER	QUESTION
6001	Do you have a Mobile Device Policy?
6002	Do you have any mobile devices accessing CJI?
6003	Do you allow the use of cellular service outside of the U.S.
6003.1	If Yes: Do you perform an inspection to ensure that all controls are in place and functioning properly in accordance with the agency's policies prior to and after deployment outside of the U.S.
6004	Does your mobile device policy dictate the use of Bluetooth and its associated devices based on the agency's operational and business processes.
6005	Do you use Mobile Hotspots? If yes, do you:
6005.1	Enable encryption on the hotspot
6005.2	Change the hotspot's default SSID
6005.3	Ensure the hotspot SSID does not identify the device make/model or agency ownership
6005.4	Create a wireless network password (Pre-shared key)
6005.5	Enable the hotspot's port filtering/blocking features if present
6005.6	Only allow connections from agency controlled devices
6005.7	OR Have a MDM solution to provide the same security as identified in items 6005.1 – 6005.6 above
6006	Do you have a Mobile Device Management (MDM) solutiuon? If Yes, do you:
6006.1	Ensure that CJI is only transferred between CJI authorized applications and storage areas of the device.
6006.2	Have a MDM with centralized administration configured and implemented to perform at least the following controls:
6006.2.1	Remote locking of device
6006.2.2	Remote wiping of device
6006.2.3	Setting and locking device configuration
6006.2.4	Detection of "rooted" and "jailbroken" devices
6006.2.5	Enforcement of folder or disk level encryption
6006.2.6	Application of mandatory policy settings on the device
6006.2.7	Detection of unauthorized configurations
6006.2.8	Detection of unauthorized software or applications
6006.2.9	Ability to determine the location of agency controlled devices
6006.2.10	Prevention of unpatched devices from accessing CJI or CJI systems
6006.2.11	Automatic device wiping after a specified number of failed access attempts
6007	Do you ensure that wireless devices (select all that apply):
6007.1	Apply available critical patches and upgrades to the operating system as soon as they become
6007.2	Are configured for local device authentication (see Section 5.13.7.1 CJIS policy)
6007.3	Use advanced authentication or CSO approved compensating controls as per Section 5.13.7.2.1 CJIS
6007.4	Encrypt all CJI resident on the device
6007.5	Erase cached information, to include authenticators (see Section 5.6.2.1) in applications, when
6007.6	Employ personal firewalls on full-featured operating system devices or run a Mobile Device
6007.7	Employ malicious code protection on full-featured operating system devices or run a MDM system
6008	Do you ensure a personal firewall is employed on all mobile devices that have a full-feature operating
6009	Does the personal firewall (select all that apply)
6009.1	Manage program access to the Internet
6009.2	Block unsolicited requests to connect to the user device.
6009.3	Filter incoming traffic by IP address or protocol.
6009.4	Filter incoming traffic by destination ports
6009.5	Maintain an IP traffic log

DESTRUCTION AND DISPOSAL

- Overwriting digital media At Least 3 times
  - This is for reuse OR release for destruction by unauthorized individuals
  - Includes hard drives from leased or rented copiers and/or printers that scanned, printed or copied CJI or PII

- Media must be disposed of or destroyed by authorized personnel
  - Either completing the action, or witnessing the action

- Must be documented
  - Policies
  - Agreements

VENDORS

- There is NO "CJIS CERTIFIED" Product!
  - State-to-state programs
  - Utah is new to state-level
  - Local environments must still be validated!

- State-Level Reviews
  - Agreements
  - Background Checks & Fingerprints
  - Review of vendor environment

- Consideration for Cloud Storage

AREAS BEING UPDATED IN 6.0 MODERNIZATION

- Cloud Computing
  - Issue: Often overlooked with 3rd party software solutions
  - Under Review: General usage requirements and Security Controls under review

- Password Standards
  - Issue: Basic Password Standards vs. Advanced Password Standards (Either/Or)
  - Under Review: Standards themselves and when to use
  - Will likely include an update to Advanced Authentication

WRAP-UP & QUESTIONS

DPS/CJIS ISO:
Lani Dick
lani@utah.gov
801-386-6964

DTS Security Partner
Roxanne Scoggan
rscoggan@utah.gov
385-254-1091