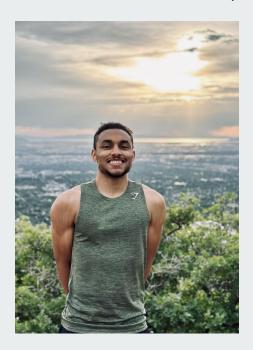
CJIS IT Security Audits

DPS CJIS Security Team

Tyson Jarrett - CJIS Information Security Officer



Jarrel Beal - Senior Business Analyst



CJIS IT Security Audits

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

Our Objectives

Measure & improve agencies' ability to provide appropriate controls to protect the full lifecycle of Criminal Justice Information.

- Oversee CJIS IT Security audits
- Establish audit schedule and scope
- Help with technical questions related to CJIS security controls
- Interpret requirements outlined in the CJIS Security Policy
- Record and track cybersecurity incidents

Agenda

- New Auditing Team
- New Audit Format
- Audit Process Timelines
- CJIS Security Policy v.5.9.2
- Q&A

New Auditing Team

Why a new auditing team?

- Knowledge of the CJIS Security Policy and expertise in all 15 policy areas
- Real-world experience in law enforcement and as CJIS policy practitioners
- Established technology & processes to create and maintain an efficient audit experience
- Proven history of conducting CJIS IT audits in other states
- Resources to effectively audit all ~600 criminal justice agencies within the 3 year cycle

Who are they?















Meet the Auditing Team



TATUN

Director of CJIS ACE

Chief ISO of Diverse Computing



COFFEE

Deputy Director- FBI Policy &
CJIS Assessments

LARRY



SIRACUSANO

Deputy Director- Audits & Strategic



KELLIE BROWN



EDITH KOWALIK CJIS Analyst I



RACHAEL VANDEUSEN

CJIS Analyst III

CJIS Analyst I

The Role of CJIS ACE

- Conduct CJIS IT audits in partnership with DPS CJIS Security team
- Primary point of contact for all audit-related inquiries
- Provide real-time guidance and feedback related to agency CJIS compliance
- Respond to technical questions related to the CJIS Security Policy
- Update DPS team with progress of ongoing audits

Benefits for Agencies

- Access to best-in-class CJIS Security expertise (Opportunities for improvement)
- More streamlined and efficient audit process and tools (Less time consuming)
- Single location for audit questionnaire and document uploads (Less confusing)
- More resources available for questions and guidance (Prompt and thorough responses)

New Audit Process

Question: By a show of hands, how many have gone through the CJIS IT Security audit before?

30
days
before
audit

Agency will be notified via email 30 days prior to their audit being issued.

21 days before audit The Pre-Audit
Questionnaire will be
issued in CJIS Audit. The
agency will have 14 days
to complete it.

14 days after audit review If there are non-compliant findings, additional responses will be required, including corrective action plans with estimated completion dates.

Audit is issued

The audit will be assigned in the 'CJIS Audit' tool.

Audit is due in 30 days Auditors will review the audit responses and the submitted documentation.

Completion of Corrective Action Plans

Auditors will follow up to ensure the corrective action plans have been completed and that your agency is now in compliance.

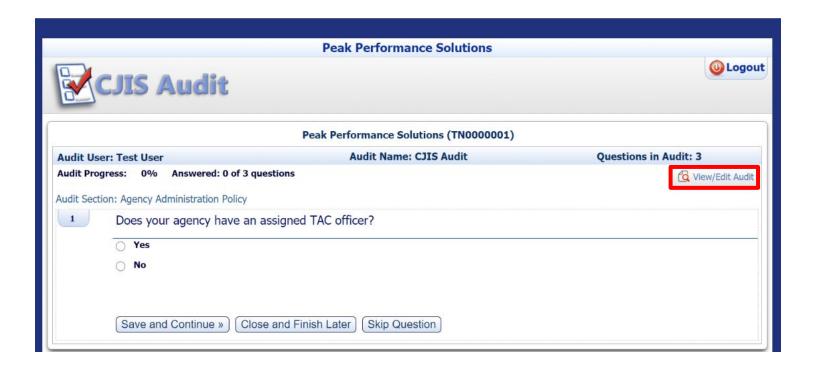
Audit Process Timeline

New Auditing Tool



All new audits moving forward will be using the tool and process discussed in this presentation.

Inside the Audit



View/Edit Audit



Viewing Audit Progress: CJIS Audit for Agency: Peak Performance Solutions

Question	User Answer	
Section: Agency Administration Policy		
Does your agency have an assigned TAC officer?	Unanswered	Answer
When you complete this electronic audit, please submit the items listed on this attachment to your auditor to finish your audit.	Unanswered	Answer
Question	User Answer	
Section: Mobile Data		
Does your agency have mobile data computer access to NCIC?	No	Re-Answe

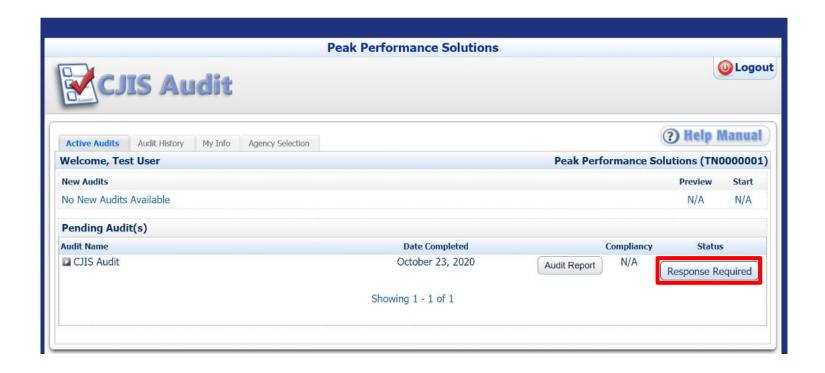
Uploading Documents



Documentation Best Practices

- Must be created by the agency and tailored to the agency's processes & procedures
- Cannot be copied from the CJIS Security Policy or a policy template
- Document title is concise and matches what is being uploaded
- Markings:
 - Official agency indication (logo or letterhead)
 - Date of creation
 - Date or frequency of review

Response Required



Next Steps

- 1. Communicate with your LASO about the audit & its requirements.
- 2. Once the audit notice is received, ensure you have a working <u>UtahID</u> account and test your ability to login to <u>CJIS Audit</u>.
- 3. Once you receive the list of documents required for the audit (currently being developed), ensure the agency's documentation, and the associated processes, are compliant and up to date.
- 4. Familiarize yourself with CJIS Security Policy requirements, specifically <u>v.5.9.2</u> updates.

CJIS Security Policy (v.5.9.2) Updates

Question: Were you aware the CJIS Security Policy was updated in December?

CJIS Security Policy v.5.9.2 Updates

Sanctionable for audit October 1, 2023

- AT (Awareness & Training)
- MP (Media Protection)
- SA (System & Services Acquisition)
- SI (System & Information Integrity)

Sanctionable for audit October 1, 2024

• IA (Identification & Authentication)

Resources

- Chris Weatherly (FBI CJIS ISO) discussing CJIS Security Policy updates
 - https://youtu.be/KGFvvngYGtl?t=1135
- Presentation from video (above)
 - https://drive.google.com/file/d/13k1QY DHkEfV7G 5cD6 jEa5N73QZgl/view?usp=drive link
- CJIS Requirements Companion Document
 - https://le.fbi.gov/cjis-division/cjis-security-policy-resource-center/requirements-companion-do cument v5-9 20200601.pdf/view

Next Steps

- 1. Collaborate with LASO and other personnel involved with policy & procedure updates
- 2. Make sure the agency's processes & policies are updated to reflect the changes in <u>v.5.9.2</u>
- 3. Establish a plan to accommodate future CJIS Security Policy modernization updates

Contact Info

For existing (V.0 & V.1) audits: Jarrel Beal - <u>jarrelbeal@utah.gov</u> / 385-253-2420

IT security questions & reporting security incidents: **Tyson Jarrett** - <u>tjarrett@utah.gov</u> / 385-255-0888



Q&A