



# 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?



CJIS ACE  
BY THE  
NUMBERS

6

EXPERTS

150

YEARS  
EXPERIENCE

46

YEARS  
EDUCATION

ACROSS

4

STATES

OVER  
200

CLIENTS

100%

CJIS READY



# Meet the Auditing Team

---



BILL  
TATUN

Director of CJIS ACE  
Chief ISO of Diverse Computing



LARRY  
COFFEE

Deputy Director- FBI Policy &  
CJIS Assessments



BROOKE LYNN  
SIRACUSANO

Deputy Director- Audits & Strategic  
CJIS Engagements



RACHAEL  
VANDEUSEN

CJIS Analyst III



KELLIE  
BROWN

CJIS Analyst I



EDITH  
KOWALIK

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?

# Audit Process Timeline

**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.



## New Auditing Tool




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

# Inside the Audit

The screenshot displays the 'Peak Performance Solutions' interface for a 'CJIS Audit'. The header includes the 'Peak Performance Solutions' title, a 'Logout' button, and the 'CJIS Audit' logo. The main content area shows the audit details: 'Peak Performance Solutions (TN0000001)', 'Audit User: Test User', 'Audit Name: CJIS Audit', and 'Questions in Audit: 3'. The audit progress is 0% with 0 of 3 questions answered. A 'View/Edit Audit' button is highlighted with a red box. The current question is 'Does your agency have an assigned TAC officer?' with radio button options for 'Yes' and 'No'. At the bottom, there are three buttons: 'Save and Continue »', 'Close and Finish Later', and 'Skip Question'.

Peak Performance Solutions

 **CJIS Audit** Logout

Peak Performance Solutions (TN0000001)

**Audit User: Test User** **Audit Name: CJIS Audit** **Questions in Audit: 3**

**Audit Progress: 0%** **Answered: 0 of 3 questions** [View/Edit Audit](#)

Audit Section: Agency Administration Policy

**1** Does your agency have an assigned TAC officer?

Yes

No

[Save and Continue »](#) [Close and Finish Later](#) [Skip Question](#)



# View/Edit Audit

 View as PDF

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

Question	User Answer
<b>Section: Agency Administration Policy</b>	
1 Does your agency have an assigned TAC officer?	Unanswered <a href="#">Answer</a>
2 When you complete this electronic audit, please submit the items listed on this attachment to your auditor to finish your audit.	Unanswered <a href="#">Answer</a>
<b>Section: Mobile Data</b>	
1 Does your agency have mobile data computer access to NCIC?	No <a href="#">Re-Answer</a>

# Uploading Documents

↳ 2. Please upload a copy of your User Agreement as a PDF.

---

**I don't have this document.**

-- Or --

Please do not upload documents that contain CJJ.

**Document Title**

**File Upload**

Choose File No file chosen

Upload

# 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

The screenshot displays the Peak Performance Solutions (PPS) CJIS Audit interface. At the top, the header includes the PPS logo, the text 'Peak Performance Solutions', and a 'Logout' button. Below the header, there are navigation tabs for 'Active Audits', 'Audit History', 'My Info', and 'Agency Selection', along with a 'Help Manual' link. The main content area is titled 'Welcome, Test User' and 'Peak Performance Solutions (TN0000001)'. It features two sections: 'New Audits' and 'Pending Audit(s)'. The 'New Audits' section shows 'No New Audits Available'. The 'Pending Audit(s)' section contains a table with one entry: 'CJIS Audit', completed on 'October 23, 2020', with a status of 'Response Required'. A red box highlights the 'Response Required' status in the table. Below the table, it indicates 'Showing 1 - 1 of 1'.

Audit Name	Date Completed	Compliance	Status
<input type="checkbox"/> CJIS Audit	October 23, 2020	<a href="#">Audit Report</a> N/A	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 [UtahID](#) account and test your ability to login to [CJIS Audit](#).
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 [v.5.9.2](#) 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](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-document\\_v5-9\\_20200601.pdf/view](https://le.fbi.gov/cjis-division/cjis-security-policy-resource-center/requirements-companion-document_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 [v.5.9.2](#)
3. Establish a plan to accommodate future CJIS Security Policy modernization updates

---

## Contact Info

For existing (V.0 & V.1) audits: **Jarrel Beal** - [jarrelbeal@utah.gov](mailto:jarrelbeal@utah.gov) / 385-253-2420

IT security questions & reporting security incidents: **Tyson Jarrett** - [tjarrett@utah.gov](mailto:tjarrett@utah.gov) / 385-255-0888



**Q&A**

---