What to Expect at an Agency Technical Security Audit ?

Stephen “Doc” Petty
CJIS Information Security Officer

CJIS Technical Audit Overview

Who, What, Why and When

Audit Process

Review Network Diagram

Review Written Policies/Process

Available Resources

Helps To Know….

Who conducts a CJIS Technical audit?

What is being audited?

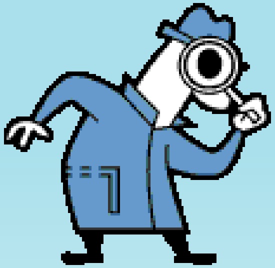
Why is the agency being audited?

When does the audit take place?

WHO CONDUCTS THE TECHNICAL SECURITY AUDIT ?

Texas DPS CJIS Security Team

- Ensures all criminal justice accessing TLETS meet requirements mandated by the CJIS Security Policy
- Support other CRS/CJIS audits on technical issues
- Office created 2005
- CJIS Information Security Officer – Stephen “Doc” Petty
- 9 Auditors
- 1,300+ TLETS agencies
- 2017 Online audit process implemented



What is being audited?

Audit of the 500+ “shall” statements in the CJIS Security Policy:

- Physical Security
- Network Diagrams
- Policies & Processes pertaining to CJI access, storage, and transmission

WHY IS THE AGENCY BEING AUDITED?

CJIS Security Policy requirement:

Once every three years

There are other audit triggers

Other audit triggers

New Agency

Security incident or exceptional event

Any physical move

Major system upgrade(s)

SECURITY AUDIT PROCESS

DPS Technical Auditor Schedules the audit:

- Phone call to agency – confirm contacts
- Walk the agency through the online audit process
- Follow up with the audit notification email to the agency detailing instructions.
- Audit is assigned and begins
- Send the following required policies/documents within 14 days:
  - –Agency Standard Operating Procedures (SOP)
  - –Account Management Process
  - –Disposal of Electronic & Physical Media
  - –Incident Response Plan
  - –Personnel Sanction Policy
  - –Security Alert & Advisory Process
  - –Security Addendum (SA)
  - –Management Control Agreement (MCA)
  - –Network Diagram

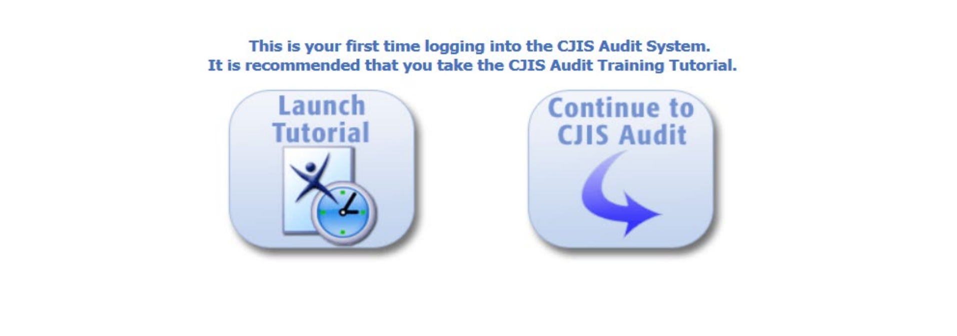
  Sample documents available here
  http://www.dps.texas.gov/SecurityReview/documents.htm

- Respond to any agency questions

The audit begins …..

1. The audit begins when the audit is assigned via the online portal

https://www.cjisportal.com/TX/security/cjisaudit/login_page.pl?USER_TYPE=TAC



This is your first time logging into the CJIS Audit System.
It is recommended that you take the CJIS Audit Training Tutorial.

2. The agency begins submitting documents/responses as indicated from the online questionnaire.

3. Respond to each question clearly. Avoid vague responses, and explain local processes, if necessary.

4. Once the agency submits the online audit, the auditor will review the answers and follow up with the agency to setup an on-site visit.

Site Visit (Audit Closeout Process)

The auditor will arrive promptly on the date and time scheduled.

Be ready, have local policies, network diagrams and related documentation on hand.

Documents to Have Available

IT / Network Support / Vendor Support:

- Signed complete Security Addendum (SA)
- Management Control Agreements (MCA)
- Inter-local agreements, MOU
- Vendor/IT Security Awareness Training list
- FIPS certificates for any encryption

Agency Personnel:

- Security Awareness Training List
- Finger prints for everyone with Access.

Documents to Have Available (cont.)

The following below may be requested at the on-site visit. Please have these items available, if needed or requested by the auditor.

- ✓ Security Awareness Training Documentation
- ✓ Incident Response Plan w/Contact Information
- ✓ Standard Operating Procedures (SOP)

  Must include processes for account management, remote access, personally owned information systems, media protection, personnel sanctions

- ✓ Mobile Policy (MDT if applicable) or BYOD
- ✓ Electronic & Physical Media Disposal
- ✓ Security Alert Process
- ✓ Network Diagram
- ✓ Memorandum of Understanding (MOU if applicable)
- ✓ FIPS Certificates (if applicable)

Find FIPS certs @ https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules/Search

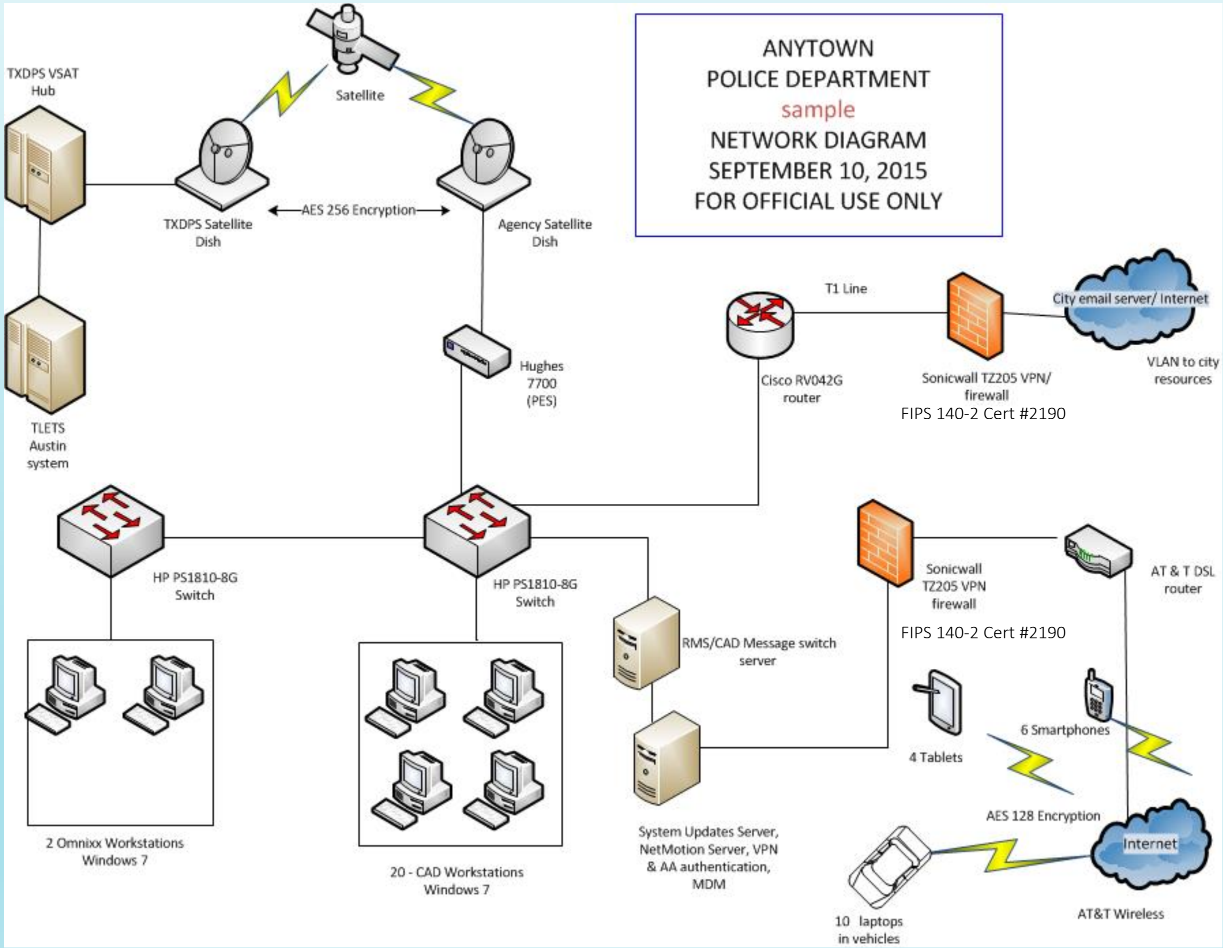
During the Site Visit

Be prepared to escort the auditor to areas within the agency. Dispatch, network closets, anywhere a terminal or access point may be located.

The auditor will indicate what areas they need to visit. This may include patrol vehicles, if MDTs are utilized.

This may include other locations (DA, Jail, LiveScan or Latent Print Device locations …)

Network Diagram



ANYTOWN
POLICE DEPARTMENT
sample
NETWORK DIAGRAM
SEPTEMBER 10, 2015
FOR OFFICIAL USE ONLY

BASIC NETWORK DIAGRAM ELEMENTS

- Depicts routers, switches and firewalls with make and model.
- Annotates the different device types (PCs, laptops, phones) with quantity.
- Network properly segmented from non-law enforcement networks.
- Firewall in place between non-LE networks and Internet.
- CJI data transmitted outside the secured network must be encrypted at a minimum of AES-128 bit and meet FIPS 140-2 standards. Certificate(s) can be found on the link below:

  https://csrc.nist.gov/Projects/cryptographic-module-validation-program/Validated-Modules/Search
- Agency name, date and For Official Use Only.

Be prepared to explain....

Any technical elements:

- VLANS, ACLs existing and how configured
- Encryption types between points
- Fiber connections
- Network segments not within the secured location
- Where CJI data is stored?
- How CJI data is protected?

Computer and Network Security

Computer Security

- Operating system patches applied are up to date.
- Anti-virus installed, functional and signature files updated.
- Session locked after 30 min of inactivity.

  Exempt from session lock (MDT's Patrol Vehicles and Dispatch)

- Terminals kept behind secure doors, protected from unauthorized viewing.
- Visitors are escorted.

Network Security

- Equipment has not met end of life (EOL).
- Equipment has patches applied and up to date.
- Equipment stored in secure area.
- Visitors are escorted.

Reviewing Vendor Software

- ✓ Software patches up to date
- ✓ CJI data transmitted outside the secured network is encrypted at a minimum 128 bit and is FIPS 140-2 certified
- ✓ Meets password requirements
- ✓ Locks after 5 consecutive invalid log on attempts
- ✓ NCIC & III transactions retained for 1 year
- ✓ Log audit events
- ✓ Meets audit retention, monitoring , alert and review requirements
- ✓ Validate where the CJI data is stored (if applicable)?
- ✓ Remote access into network has Advanced Authentication and meets encryption requirements

Physical Security

- Physical locks, doors and windows. Entry and exit secured.
- Challenge and identification of visitors. Authentication.
- Terminal Location. Positioned Securely.
- Session Lock, screen saver methods for securing terminals.
- Mobile Units, secured in lockable vehicle, ensure screen is not viewable
- Network / Equipment Room Locks
- Access Points , location and accessibility
- Offsite Areas (if applicable / media storage, communication equipment)

Reviewing Laptops

- Operating system patches applied are up to date.
- Firewall installed/turned on and Anti-Virus up to date.
- Advanced Authentication (AA) being utilized outside the secure location.
- If required, encryption in use, FIPS certificates.
- List of devices (Aircards, etc).
- Incident Response Plan addressing device loss.
- Any policies addressing usage outside the secured location.
- Any Bring Your Own Device (BYOD) policies in place.

Reviewing Mobiles

- Advanced Authentication (AA) being utilized outside the secure location.
- If requested, Compensating Controls for AA email on file.
- Mobile Device Management (MDM) in place for tablets and phones.
- Incident Response Plan addressing mobile device loss.
- Any policies addressing usage outside the secured location.
- Any Bring Your Own Device (BYOD) policies in place.

Audit Closeout

The auditor will discuss any areas of weakness or non-compliance.

Feel free to ask questions or request clarification of any items in question.

Our goal is to ensure security and compliance; we can help you to identify weak areas.

Audit Process - Compliant

Formal email to agency

Review findings in CJIS Audit portal

Next scheduled security review in 3 years

AUDIT PROCESS – NON-COMPLIANT

Formal Non-compliant email

Agency given 30 days to correct non-compliant issues **<u>or</u>** submit plan for correcting items

Once all identified non-compliance issues have been resolved and verified with the auditor, an updated full compliant notice will be provided to the agency and updated within the audit records/portal.

Available Resources
Security Review Website

http://www.dps.texas.gov/securityreview

CJIS Security Policy
Security Awareness Training Resources
System Access
Network Diagram Examples
Management Control Agreement
CJIS Security Addendum
Security Newsletters
Links for Cyber Training and LEEP info
ListServ signup on bottom of home page

CJIS Audit Team

Texas CJIS ISO, Stephen "Doc" Petty (512) 424-7186

James Buggs CJIS Auditor II (512) 424-7794	Jeannette Cardenas CJIS Auditor II (512) 424-7910	Daniel Conte Lead Technical Auditor (512) 424-7137
Oswald Enriquez CJIS Auditor II (512) 424-7914	William Gore CJIS Auditor II (512) 424-7401	James Gore CJIS Auditor II (512) 424-7911
Linda Sims CJIS Auditor II (512) 424-2937	Sonya Stell CJIS Auditor II (512) 424-2450	Deborah Wright Lead Technical Auditor (512) 424-7876
Security.Committee@dps.texas.gov		

CJIS Security Office

Texas Department of Public Safety
CJIS Technical Security Team
512-424-5686
security.committee@dps.texas.gov

Questions?