



WHAT TO EXPECT @ A TECHNICAL SECURITY AUDIT

Alan Ferretti
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 are you 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 – Alan Ferretti
- 10 Auditors
- 1,200+ TLETS agencies



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.

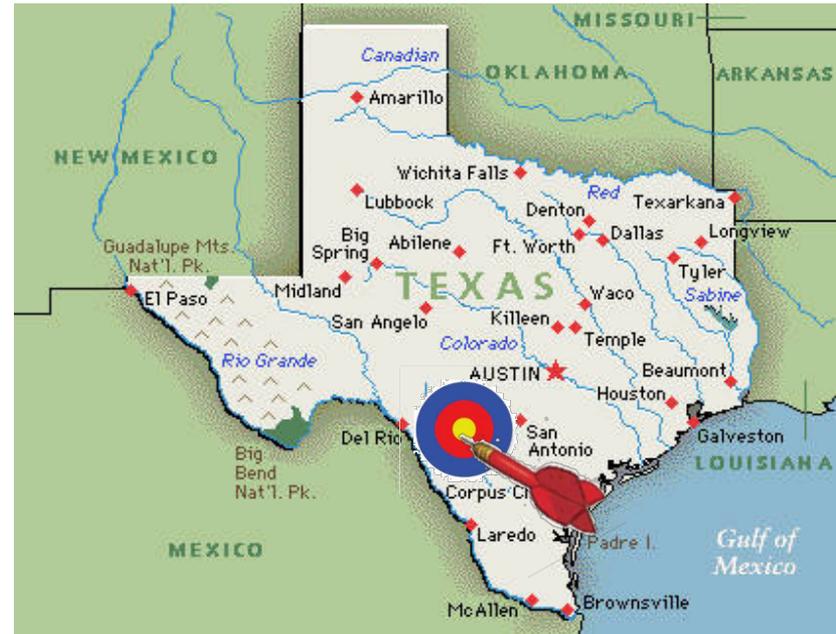


WHY IS THE AGENCY BEING AUDITED?

CJIS Security Policy
requirement:

Once every three years

There are other audit
triggers



Other audit triggers

New Agency

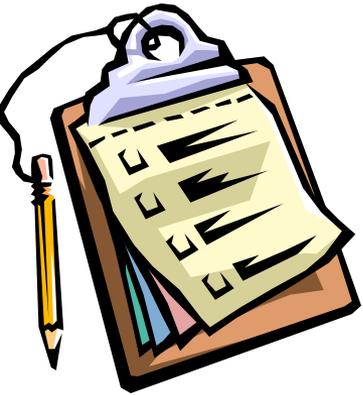
Security incident or exceptional event

Any physical move

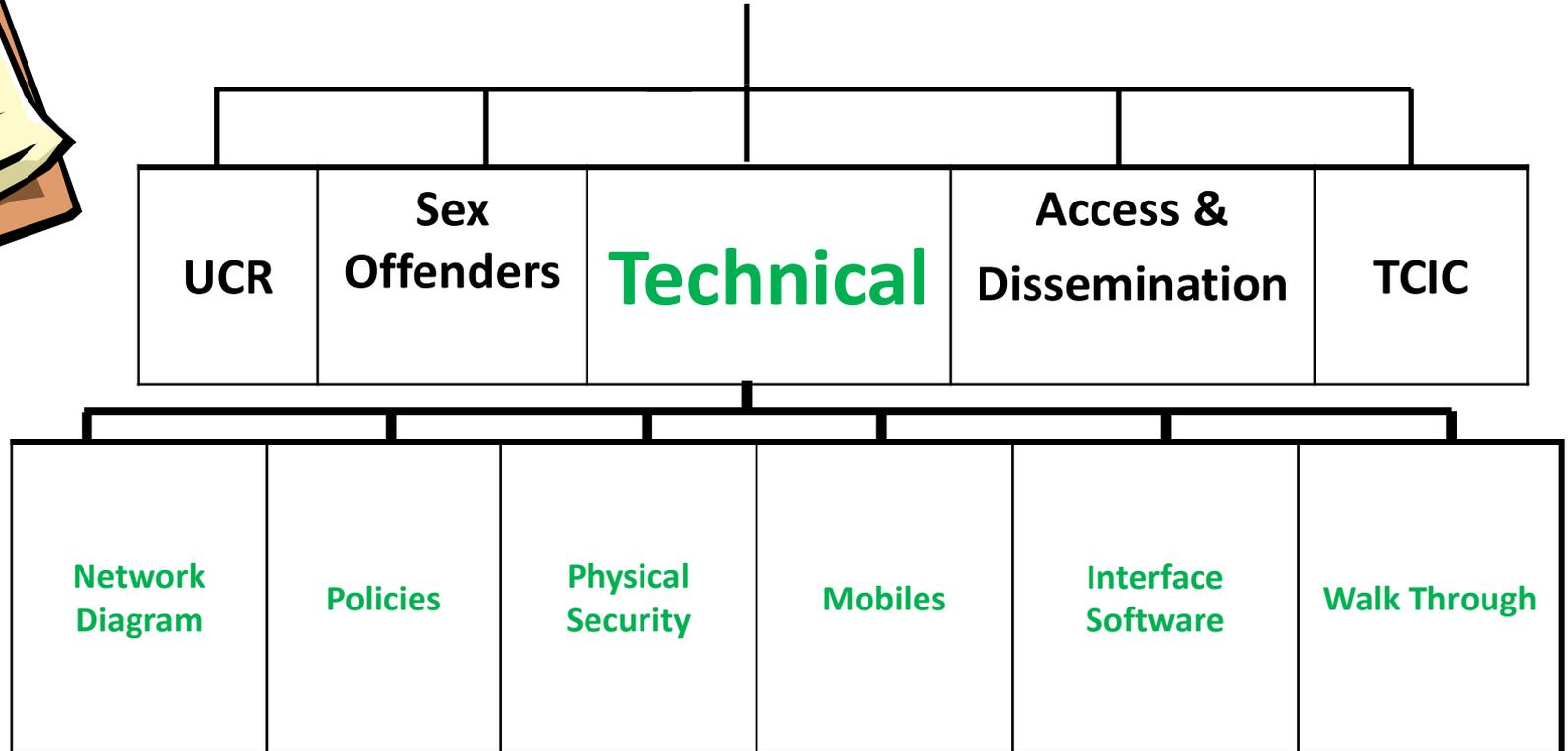
Major system upgrade exceeding 25 % change from the original system



What is included in the audit?



FBI & DPS Audit Programs



SECURITY AUDIT PROCESS

DPS Technical Auditor Schedules the audit

- 2 - 4 weeks notice when possible
- Phone call to agency – Set date and time, confirm contacts.
- Follow up with email to the Agency detailing instructions and send samples of following required policies:
 - Agency Standard Operating Procedures (SOP)
 - CJIS Security Audit - BLANK COPY
 - CJIS Security Policy - CURRENT VERSION
 - Disposal of Electronic & Physical Media
 - Incident Response Plan
 - Security Alert & Advisory Process
 - Security Addendum
 - Security Awareness Training - PDF REVIEW MATERIAL
- Respond to any agency questions



AUDITOR ARRIVES ON SITE

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

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



The audit begins

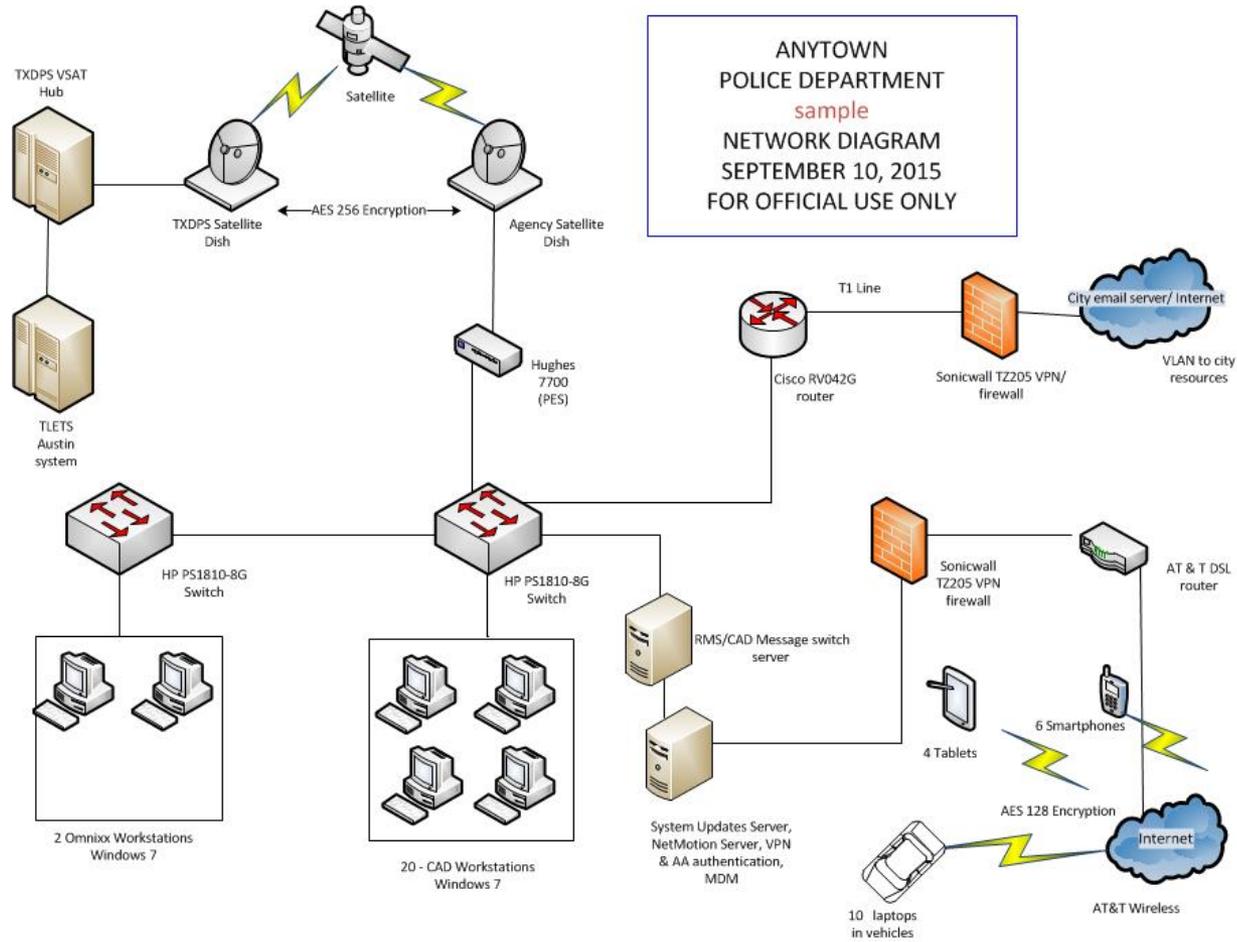
The auditor will introduce themselves.

Ensure necessary staff are present. This may include IT Support, Administrative, and Managerial Personnel.

The Audit will cover all areas of the CJIS Security Policy. Have a copy of the audit form available to follow along.

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





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.

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?



Start gathering information

IT /Network Support / Vendor Support

Signed complete Security Addendum

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.



Paperwork to have ready at audit

Management Control Agreements / Security Addendums

Security Awareness Training Documentation

Incident Response 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)



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.

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

CJI data stored where?

Remote access into network has Advanced Authentication and meets encryption requirements



SITE INSPECTION

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, ...)



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 into enclosed vehicle, screen viewable

Network / Equipment Room Locks

Access Points , location and accessibility

Offsite Areas (if applicable / media storage, communication equipment)



Reviewing Laptops

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.



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

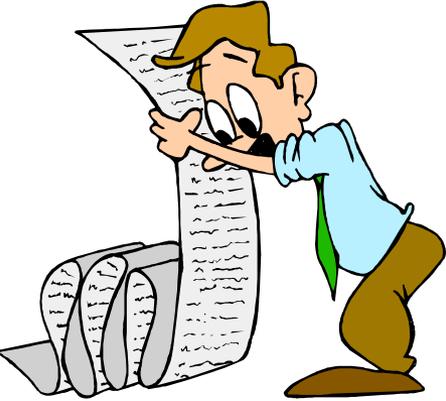


Formal email to agency

Next scheduled security review in 3 years



AUDIT PROCESS – NON-COMPLIANT



Non-compliant email listing items found

Agency given 30 days to correct non-compliant issues or submit plan for correcting items

Compliant email sent to agency upon verification of corrected items



Texas Audit Statistics

In the 12 months ending August 31, 2014:

There were 67 “new” agencies added for Audit.
Current Total Agencies we audit is 1,227.

Technical Security Auditors drove 99,310 miles.
There were no accidents (Or speeding tickets)

Completed 436 Technical Audits:

218 were Compliant

124 became Compliant

94 are still working issues



Top Reasons for non-compliance:

Software, Patches, Updates

Remote Support - Encryption/AA

Security Awareness Training

Local Agency Required Policies



Available Resources

Security Review Website

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

CJIS Security Policy
Security Awareness Training Resources
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, Alan Ferretti (512) 424-7186

Chip Burleson CJIS Auditor (512) 424-7401	Jeannette Cardenas CJIS Auditor (512) 424-7910	(Open Position)
Daniel Conte CJIS Auditor (512) 424-7137	Oswald Enriquez CJIS Auditor (512) 424-7914	Stephen 'Doc' Petty CJIS Auditor (512) 424-7055
Erwin Pruneda CJIS Auditor (512) 424-7911	Linda Sims CJIS Auditor (512) 424-2937	Deborah Wright Lead Tech. Auditor (512) 424-7876
firstname.lastname@dps.texas.gov		



CJIS Security Office

Texas Department of Public Safety

CJIS Technical Security Team

512-424-5686

security.committee@dps.texas.gov



Questions?

