CJIS SECURITY POLICY v5.7

Stephen “Doc” Petty,
CJIS ISO - Texas

Agenda

- Overview CJIS & APB
- Highlight Current Policy & Changes
- Audit Process - What to Expect
- LiveScan & IOT
- Texas Audit Statistics
- Resources & Questions

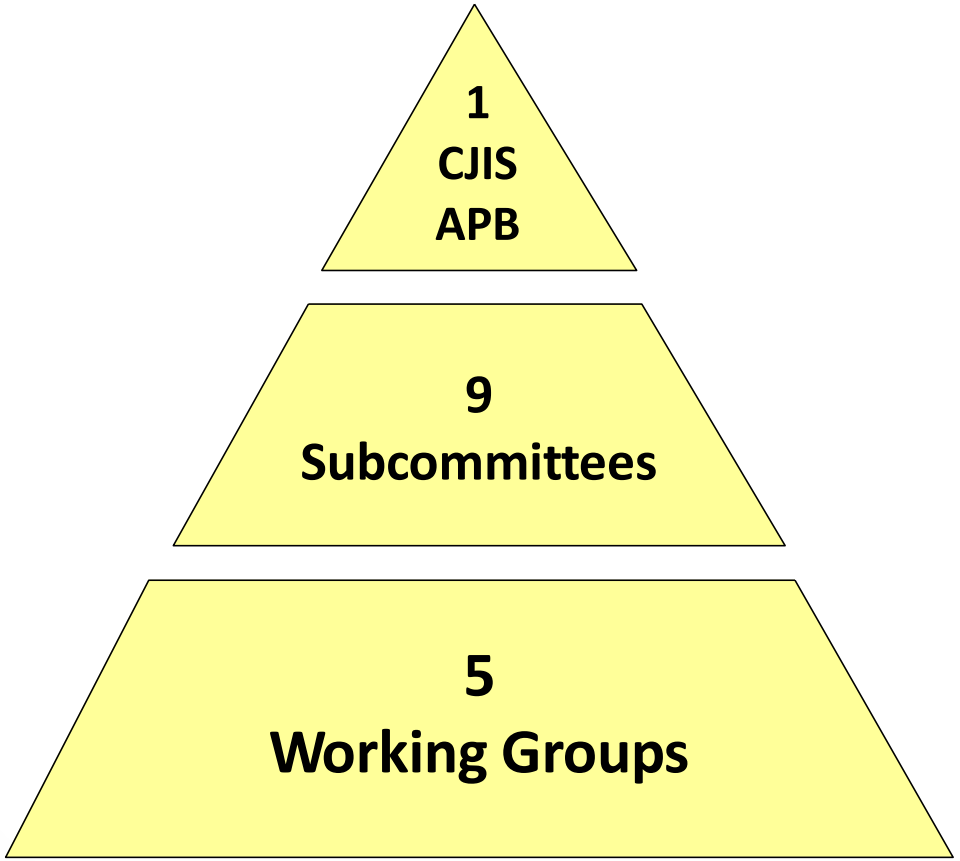
Shared Management Philosophy

- The FBI employs a shared management philosophy: Federal Law Enforcement, Local Law Enforcement, State Law Enforcement, & Tribal Law Enforcement

- Similar relationship with the Compact Council and State Identification Bureaus: Noncriminal justice usage of criminal history records

- The Advisory Process Board, subcommittees, and working groups, collaborate with the FBI CJIS division to ensure that the CJIS Security Policy meets the evolving business, technology, and security needs.

CJIS SECURITY POLICY



The Advisory Policy Process

Two Cycles Annually

- Topic Papers (Discussion items submitted)
- Spring and Fall (APB Meets)
- Working Groups, Subcommittees, Board
- FBI Director (Approval and sign off on Policy)

U. S. Department of Justice
Federal Bureau of Investigation
Criminal Justice Information Services Division

Criminal Justice Information Services (CJIS) Security Policy

Version 5.7
08/16/2018

CJISD-ITS-DOC-08140-5.7

Prepared by:
CJIS Information Security Officer

Approved by:
CJIS Advisory Policy Board

CJIS Technical Audit

Policy Areas

13 Specific Policy Areas involving a Technical Audit

Policy Area 1

Information Exchange Agreements

- MCA – Management Control Agreement
- Security Addendum
- MOU – Interagency Agreements

Policy Area 2

Security Awareness Training

- Required within 6 Months, renew every 2 Years
- Awareness Topics depend on level of Access
- CJIS Online, PDF for Levels I, II & III
- Other Methods if it meets points outlined
- Must be documented / Maintained by Agency

- **Level 1**:

Personnel with unescorted access to secure areas

- **Level 2**:

Personnel that have physical contact with CJI

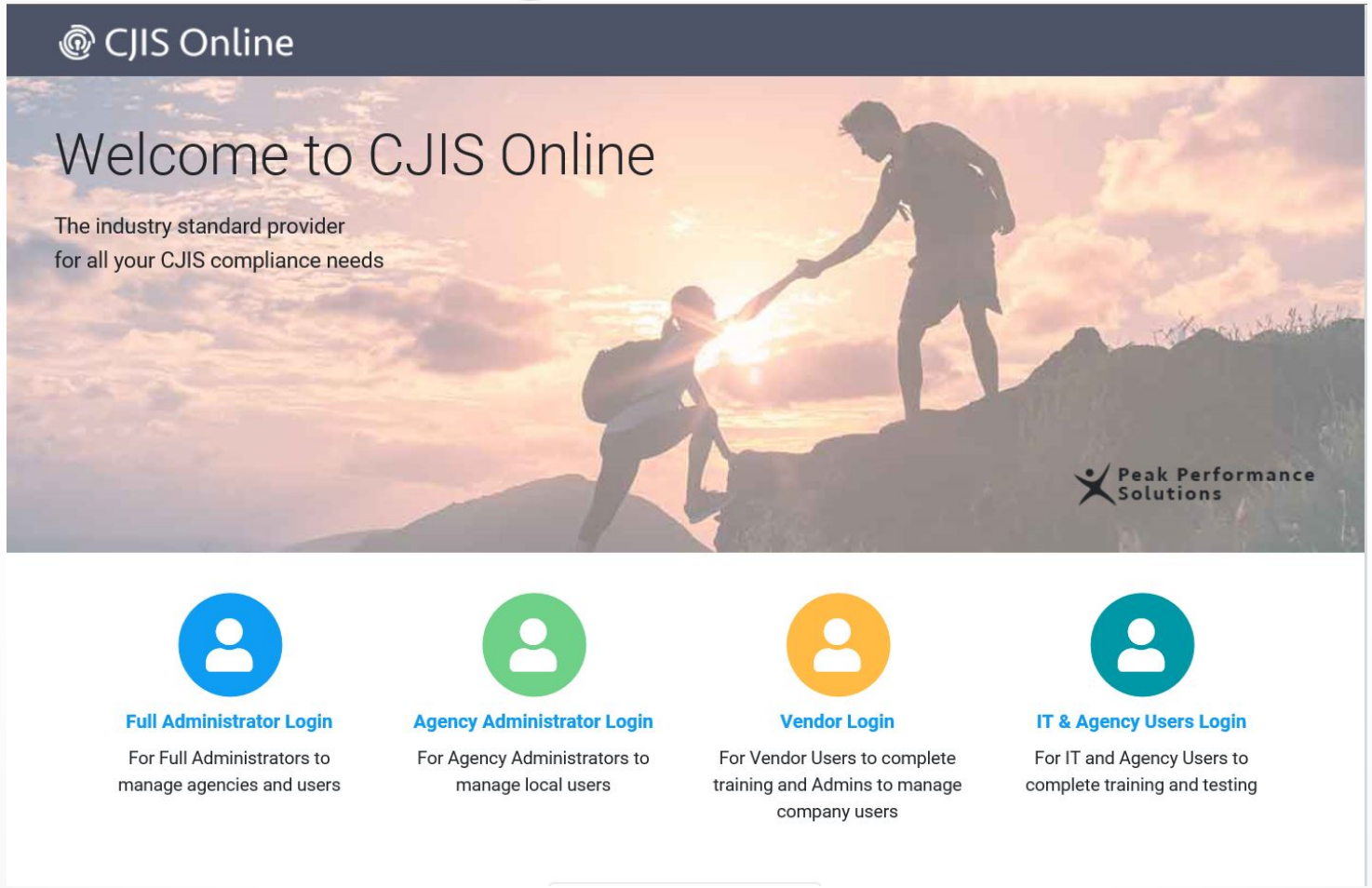
- **Level 3**:

Personnel that enter, query or modify CJI

- **Level 4**:

Personnel with Information Technology roles

Security Awareness



Policy Area 3

Incident Response

Changes in 5.5 - Section 5.13 Policy Area 13: Mobile Devices: modify language throughout the entire section based on Mobile Security Task Force recommendations

Incident Response

TEXAS CJIS SECURITY OFFICER (ISO)
COMPUTER SECURITY INCIDENT RESPONSE CAPABILITY (CSIRC)
REPORTING FORM

DATE OF REPORT (MM//DD/YYYY):_____

DATE OF INCIDENT (MM/DD/YYYY):_____

POINT(S) OF CONTACT:_____

PHONE/EXT/E-MAIL:_____

LOCATION(S) OF INCIDENT:_____

SYSTEM(S) AFFECTED:_____

_____

AFFECTED SYSTEM(S) DESCRIPTION (e.g. CAD, RMS, file server, etc.):_____

_____

METHOD OF DETECTION:_____

NATURE OF INCIDENT:_____

_____

INCIDENT DESCRIPTION:_____

_____

ACTIONS TAKEN/RESOLUTION:_____

_____

Copies to:

Stephen "Doc" Petty
Texas CJIS ISO
5805 N Lamar Blvd
Austin, TX 78765-4143
Stephen.Petty@dps.texas.gov

Michelle Farris
CRS Deputy Administrator
5805 N Lamar Blvd
Austin, TX 78765-4143
Michelle.Farris@dps.texas.gov

Policy Area 4

Auditing & Accountability

- Event Logging
- Content
- Review

Policy Area 5

Access Control

- Account Management
- Access Enforcement
- Unsuccessful Login Attempts
- System Use Notification
- Session Lock
- Remote Access
- Personally Owned Information Systems (BYOD)
- No CJI from Publicly Accessible Computers

Policy Area 6

Identification & Authentication

- Password Requirements
- PIN Numbers
- OTP (One Time Passcodes)
- AA (Advanced Authentication)

Policy Area 7

Configuration & Management

- Network Diagram
- Access Restrictions /Least Functionality
- Include connected systems; LiveScan, Latent Print

Policy Area 8

Media Protection

- Electronic
- Physical (Paper)

Policy Area 9

Physical Protection

- Secure Facility
- Controlled Area

Policy Area 10

Systems & Communications Protection and Information Integrity

FIPS 140-2 Encryption Certificates

Cloud Computing

Data "At Rest" symmetric cipher that is FIPS 197 certified (AES) and at least 256 bit strength.

Changes in 5.7 - Section 5.10.1.5 Cloud Computing: CJIS Security Policy Restriction for Criminal Justice Information Stored in Offshore Cloud Computing Facilities.

Cloud Computing

Policy Area 11

Formal Audits

- At a minimum, triennially audit all CJAs and NCJAs which have direct access to the state system in order to ensure compliance with applicable statutes, regulations and policies.

Policy Area 12

Personnel Security

- Personnel Sanction Policy
- Procedures /Forms requesting /removing access
- Physical protections access policy

Changes in 5.7 - Section 5.12.1 Personnel Security Policy and Procedures: rename section to "Personnel Screening Requirements for Individuals Requiring Unescorted Access to Unencrypted CJI" and combine previous Sections 5.12.1.1 and 5.12.1.2 into the single section.

Policy Area 13

Mobile Devices

- MDT Policy
- MDM

Live Scan & IOT

CJIS Definition

- **Criminal Justice Information (CJI)** — Criminal Justice Information is the abstract term used to refer to all of the FBI CJIS provided data necessary for law enforcement agencies to perform their mission and enforce the laws, including but not limited to: biometric, identity history, person, organization, property (when accompanied by any personally identifiable information), and case/incident history data. In addition, CJI refers to the FBI CJIS-provided data necessary for civil agencies to perform their mission; including, but not limited to data used to make hiring decisions. The following type of data are exempt from the protection levels required for CJI: transaction control type numbers (e.g. ORI, NIC, UCN, etc.) when not accompanied by information that reveals CJI or PII.

Texas Audit Statistics

- 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 ISO Plus 9 Auditors for the State of Texas
- 1,300+ TLETS agencies
- 2017 Online audit process implemented

Texas Audit Statistics

- 391 Agencies Audited for Calendar Year 2018
- Total Miles Driven by Auditors: 63,905
- 223 Agencies In Compliance at time of Audit
- 86 Agencies Became Compliant after Remediation
- 82 Agencies continuing remediation efforts or have been disconnected / taken out of service.
- As technology evolves, so too does the scope of CSP

Texas Audit Statistics

Most Common Findings in Texas Agencies:

- Written Policies (Really?)
- Patching / Malware Updates
- Encryption
- AA
- Segmentation

Texas Audit Statistics

Incident Reporting:

- Total Reported in 2018 Calendar Year: 8
- Malware/Trojans & Worms
- Command & Control Rootkits
- Lost / Stolen Devices (Handhelds – Tablets)
- Ransomware

Resources

Texas Department of Public Safety
Courtesy ~ Service ~ Protection

DPS HOME | SERVICES | EMPLOYMENT | ABOUT US

Select Language | Search DPS

Security Review

- Home
- News & Updates
- Documents
- Resources
- Training
- Security Awareness Training
- FAQs
- Contact Us

Contact Us

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

Deborah Wright, CJIS Technical Team Lead (512) 424-7876

CJIS Technical Auditors

James Buggs (512) 424-7794

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

James Gore (512) 424-7911
Linda Sims (512) 424-2937
Sonya Stell (512) 424-2450

Fax Number (512) 424-5599

Email Security Committee

via USPS:
Texas Department of Public Safety
CJIS Security Office, Crime Records
PO Box 4143, MSC 214
Austin, TX 78765-4143

via overnight carrier:
Texas Department of Public Safety
CJIS Security Office, Crime Records
5805 N Lamar Blvd, MSC 214
Austin, TX 78752

Questions?

Stephen “Doc” Petty, CISSP, SSCP
CJIS ISO - Texas
Stephen.petty@dps.texas.gov

Thank you

TEXAS
DEPARTMENT OF PUBLIC SAFETY
CRIME RECORDS
LAW ENFORCEMENT SUPPORT DIVISION