CRIMINAL JUSTICE INFORMATION SERVICES

Alan Ferretti
CJIS Information Security Officer

AGENDA

- What is CJIS?
- What is the APB?
- What is new in the latest version of the CJIS Security Policy?
- Advanced Authentication change
- Mobile policy for Tablets and Smartphones
- Cloud Computing
- Texas Audit Statistics

What is CJIS?

Criminal Justice Information Services (CJIS) is a division of the FBI located in Clarksburg, WV.

- NCIC: National Crime Information Center
  An electronic clearinghouse of crime data available 24/7.
- Crime Statistics/UCR
  Crime in the U.S
- Fingerprints and Other Biometrics
  IAFIS, Next Generation Identification, global initiatives, etc.
- LEEP: Law Enforcement Enterprise Portal
  Includes Law Enforcement Online (LEO).
- N-DEx: National Data Exchange
  An automated system for sharing information, connecting dots.
- National Instant Criminal Background Check System
  Gun Checks. Enabling safe, legal purchases of weapons and explosives.

CODE OF FEDERAL REGULATIONS
TITLE 28--JUDICIAL ADMINISTRATION
PART 20--CRIMINAL JUSTICE INFORMATION SYSTEMS

Criminal Justice Information may only be used for Criminal Justice purposes by a Criminal Justice Agency.

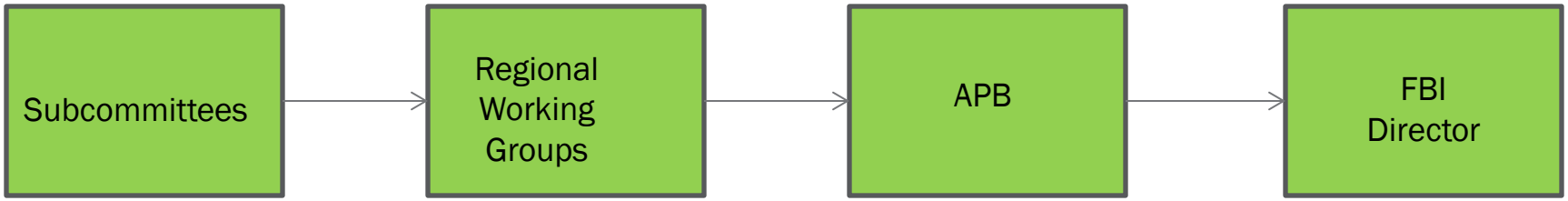
A Vendor may have access to provide support to a Criminal Justice Agency with an executed Security Addendum.

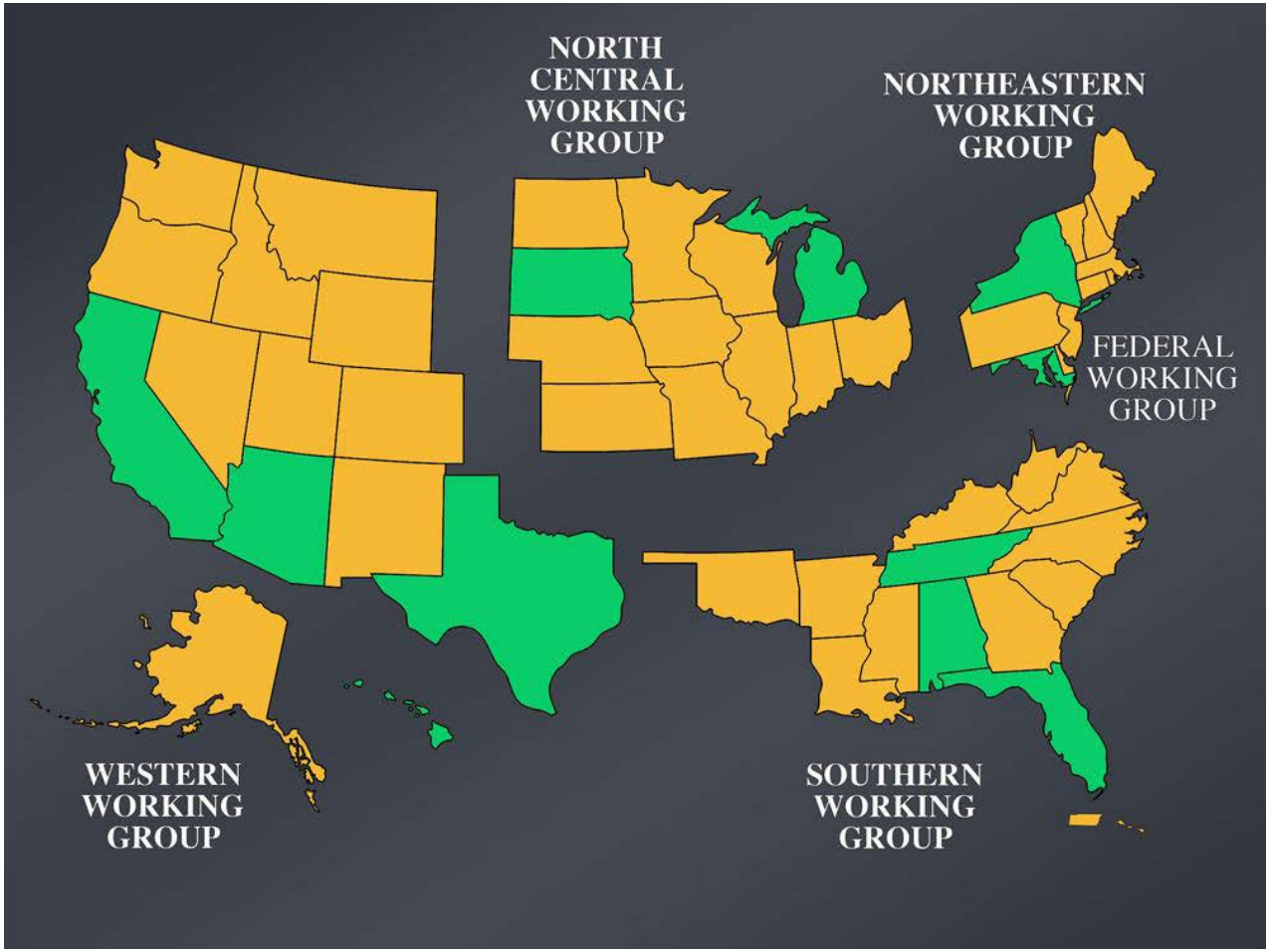
A Governmental agency may have access to provide support to a Criminal Justice Agency with a Management Control Agreement (MCA).

What is the Advisory Policy Board?

FBI Director Louis J. Freeh established the CJIS Advisory Process in the fall of 1994 and installed the CJIS Advisory Policy Board (APB) on December 15, 1994. This new CJIS Advisory Process was established to provide advice and guidance on all CJIS Division programs.

The APB is responsible for reviewing appropriate policy, technical, and operational issues related to CJIS Division programs. Subsequent to their review, the Board makes recommendations to the Director of the FBI.





Security and Access Subcommittee (S+A)
Representation:

Chairman: Alan Ferretti – TX
Vice Chair: Jeff Matthews – AL
Brenda Abaya – HI
Larry Coffee – FL
Joe Dominic – CA
Troy Goodman – MD
Blaine Koops – MI
Yosef Lehrman – NY
Bill Phillips – AZ
Charles Shaffer – FL
TJ Smith – CA
Delton Tipton – SD
Brad Truitt – TN

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

Criminal Justice Information Services (CJIS) Security Policy

Version 5.3
8/4/2014

CJISD-ITS-DOC-08140-5.3

Prepared by:
CJIS Information Security Officer

Approved by:
CJIS Advisory Policy Board

What's new in version 5.3

Updated Restricted Files

Advanced Authentication (Police Vehicles)

Advanced Authentication (Compensating Controls)

AA Decision Tree updated

Indirect Access

Session Lock Exemption

Personal Identification Numbers (PIN's)

CJI at rest encryption exception

New Policy Area – Section 5.13 Mobile Devices

Terms and Definitions updated (Appendix A)

Section 5.9.1 Physically Secure Location

"A physically secure location is a facility, ***a police vehicle,*** or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems."

Secure Locations

DEPARTMENT OF PUBLIC SAFETY
TEXAS
COURTESY · SERVICE · PROTECTION

NOT Secure Locations (AA required)

5.13.3 Wireless Device Risk Mitigations

Organizations shall, at a minimum, ensure that cellular wireless devices:

1. Apply available critical patches and upgrades to the operating system as soon as they become available for the device and after necessary testing as described in Section 5.10.4.1.

2. Are configured for local device authentication (see Section 5.13.9.1).

3. Use advanced authentication.

4. Encrypt all CJI resident on the device.

5. Erase cached information, to include authenticators (see Section 5.6.2.1) in applications, when session is terminated.

6. Employ personal firewalls or run a Mobile Device Management (MDM) system that facilitates the ability to provide firewall services from the agency level.

7. Employ antivirus software or run a MDM system that facilitates the ability to provide antivirus services from the agency level.

Addition of *COMPENSATING CONTROLS* for AA

Applies only to smartphones and tablets

Possession of agency issued device is a required part of control

Additional requirements mostly met by MDM

CSO approval and support required

What is Cloud Computing?

Defined by the CJIS Security Policy as: *A distributed computing model that permits on-demand network access to a shared pool of configurable computing resources (i.e., networks, servers, storage, applications, and services), software, and information.*

Can an Agency be compliant with the CSP and also cloud compute?

Yes - Because the CSP is device and architecture independent (per CSP Section 2.2), the answer is yes, and this can be accomplished— assuming the vendor of the cloud technology is able to meet the existing requirements of the CSP.

Cloud Computing and the CJIS Security Policy

Section 5.10.1.5 Cloud Computing

The metadata derived from CJI shall not be used by any cloud service provider for any purposes.

The cloud service provider shall be prohibited from scanning any email or data files for the purpose of building analytics, data mining, advertising, or improving the services provided.

Also see:

Appendix G.3 Cloud Computing White Paper

The IACP “Guiding Principles on Cloud Computing in Law Enforcement”.

Cloud Computing and the CJIS Security Policy

IACP Guiding Principles on Cloud Computing in Law Enforcement.

1. FBI CJIS Security Policy Compliance
2. Data Ownership
3. Impermissibility of data mining
4. Auditing
5. Portability and interoperability
6. Integrity of Data
7. Survivability of Agreement
8. Confidentiality
9. Availability, Reliability, and Performance
10. Cost- Total Cost of Ownership

Where are we in Texas

Google – no interest shown in being compliant. Data is required to be encrypted if sent to, while resident in, and returned from the "Cloud". Agency must control encryption keys.

Microsoft – Office 365 being used across the State (Country). Microsoft is about to roll out a compliant product, Azure, through DIR, that will allow for cloud based storage of large data files. Same methods as 0365 but different data centers. Total Government Cloud data centers will be at five.

AWS (Amazon) – had first meeting with DPS regarding CJIS compliance. 8/29/2014. They provide storage and expect all sensitive data to be encrypted and controlled by the owner.

There are other Cloud Providers than have been found to be CJIS compliant.

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

Alan Ferretti

(512) 424-7186

alan.ferretti@dps.texas.gov

Web Site

www.dps.texas.gov/securityreview

Questions?


DEPARTMENT OF PUBLIC SAFETY
TEXAS
COURTESY · SERVICE · PROTECTION