CJIS Security Policy:

Version 5.2 and Beyond
New Technology for
Texas Law Enforcement

Alan Ferretti
CJIS Information Security Officer
Texas Department of Public Safety

CJIS Security Policy version 5.2:

On 8/9/2013 the FBI CJIS ISO released Version 5.2 of the CJIS Security Policy (CSP).

This updated version incorporates the changes approved by the Advisory Policy Board (APB) going back to the June 2012 meeting.

You can view/download the policy and the Requirements and Transition document at:

www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view

or

www.dps.texas.gov/securityreview

Agenda:

CJIS Security Policy 5.2 changes

- Visitor Logs
- Transaction Control Numbers exemption
- Smart Phones and Tablets
- Mobile Device Management
- Cloud Computing
- Next Version (5.3) changes
- New Audit Questions
- Future Policy discussions

Visitor Log and Transaction Numbers:

Visitor Logs

The requirements for Agencies to keep a visitor log for Secure Locations has been removed.

Transaction Numbers

The following type of data are exempt from the protection levels required for CJI: transaction control type numbers (e.g., ORI, NIC, FNU, etc.) when not accompanied by information that reveals CJI or PII.

Cellular Devices:

5.5.7.3.1 Cellular Risk Mitigations

Organizations shall, at a minimum, ensure that cellular 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.
3. Use advanced authentication.
4. Encrypt all CJI resident on the device.
5. Erase cached information 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.

Mobile Device Management (MDM):

5.5.7.3.3 Mobile Device Management (MDM)

MDM facilitates the implementation of sound security controls for mobile devices and allows for centralized oversight of configuration control, application usage, and device protection and recovery [if so desired by the agency].

Devices that have been rooted, jailbroken, or have had any unauthorized changes made to them shall not be used to process, store, or transmit CJI data at any time. In addition to the security controls described in this Policy, agencies shall implement the following controls when allowing CJI access from cell/smart phones and tablet devices:

1. CJI is only transferred between CJI authorized applications and storage areas of the device.
2. MDM with centralized administration capable of at least:
    - **i. Remote locking of device**
    - **ii. Remote wiping of device**
    - **iii. Setting and locking device configuration**
    - **iv. Detection of “rooted” and “jailbroken” devices**
    - **v. Enforce folder or disk level encryption**

Policy for Cloud Computing:

5.10.1.5 Cloud Computing

Organizations transitioning to a cloud environment are presented unique opportunities and challenges (e.g., purported cost savings and increased efficiencies versus a loss of control over the data). Reviewing the cloud computing white paper (Appendix G.3), the cloud assessment located within the security policy resource center on FBI.gov, NIST Special Publications (800-144, 800-145, and 800-146),as well as the cloud provider's policies and capabilities will enable organizations to make informed decisions on whether or not the cloud provider can offer service that maintains compliance with the requirements of the CJIS Security Policy.

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.

Cloud Resources:

For Law Enforcement data/CJI:

The CJIS Security Policy and the White Paper in Appendix G.3

The cloud assessment located within the security policy resource center on FBI.gov

DPS Security Website – IACP's Guiding Principles on Cloud Computing in Law Enforcement, also available on the IACP web site.

Cloud Road Map:

For Law Enforcement data/CJI – a <u>possible</u> path to the Cloud.

Phase one could be moving email, word processing, spreadsheets and so on into the Cloud.

Phase two could be to do file storage in the Cloud. (data backups and crime scene photographs, ……..)

Phase three could be moving the Record Management System (RMS) and associated storage into the Cloud.

Phase four could be moving Computer Aided Dispatch (CAD) to the Cloud.

Upcoming Changes:

At the June 2013 meeting of the APB, two changes were approved that have impact on all Texas agencies.

It should be noted that these are not in policy until the FBI Director signs off on version 5.3 this year.

Both changes have financial consequences to Texas Agencies.

My auditors will be auditing to these standards now.

The areas are:

Secure Locations (AA requirement for police vehicles)

Compensating Controls for Smart Phones/Tablets.

Secure Location:

New Policy definition of a Secure Location

5.9.1 Physically Secure Location

(paragraph 1) 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 ...

Additionally, the APB struck the following from the policy....

Removed from Secure Location:

5.9.1 (paragraph 3) ~~For interim compliance, and for the sole purpose of meeting the advanced authentication policy, a police vehicle shall be considered a physically secure location until September 30th, 2013. For the purposes...~~

5.6.2.2.1 ~~INTERIM COMPLIANCE:~~

~~For interim compliance, users accessing CJI from devices associated with, and located within, a police vehicle are exempt from the AA requirement until September 30th, 2013 if the information system being used has not been procured or upgraded anytime after September 30th, 2005. For the purposes of this policy, a police vehicle is defined as an enclosed criminal justice conveyance with the capability to comply, during operational periods, with Section 5.9.1.3.~~

Secure Location:

What does this mean in Texas –

If a laptop is used within a police vehicle, Advanced Authentication (AA) is not required. If it is taken outside the vehicle, AA is required.

The agency must have a lock on the laptop preventing its removal or a policy against officers using the laptop outside the police vehicle.

Those agencies with AA in place may use the laptops anywhere.

We will ask for the policy or ask to see the locks during the audit.

Smart Phones and Tablets:

Reminder:

At the June 2013 meeting of the APB, two changes were approved that have impact on all Texas agencies.

It should be noted that these are not in policy until the FBI Director signs off on version 5.3 This year.

Both changes have financial consequences to Texas Agencies.

My auditors will be auditing to these standards now.

Smart Phones and Tablets:

The APB has passed a Compensating Controls for Advanced Authentication policy for use with Agency issued and controlled Smart phone or Tablets. The compensating controls may be used under these very specific conditions in lieu of Advanced Authentication for these types of devices in the State of Texas.

Translation – you may **NOT** need AA on a Smart Phone or Tablet.

Smart Phones and Tablets:

Conditions must be met:

1. The Smart phone or Tablet must be Agency owned.
2. Mobile Device Management software must be implemented to control these devices.
3. A minimum of four of the compensating controls listed in the policy must be implemented. (The policy requires 2 – we require 4 in Texas)
4. Approval of the Texas CSO must be obtained.

Compensating Controls:

What are the Compensating Controls?

- Possession of the agency issued smart phone as an indication it's the authorized user
- Implement password protection on the Mobile Device Management application and/or
secure container where the authentication application is stored
- Enable remote device locking
- Enable remote data deletion
- Enable automatic data wipe after predetermined number of failed authentication attempts
- Remote device location (GPS) tracking
- Require CJIS Security Policy compliant password to access the device
- Use of device certificates

Any 4 of the above 8 allows you to ask for an AA exemption on Smart Phones or Tablets.

Compensating Controls:

How do you get CSO approval for Compensating Controls?

The Smartphone or Tablet must be Agency owned.

Mobile Device Management software must be implemented to control these devices.

A minimum of four of the listed examples in the policy must be implemented.

An email sent to securitycommittee@dps.texas.gov (Keep a copy for your records).

You will not receive a reply.

If the above process is completed, it will result in conditional approval of your compensating controls for Advanced Authentication until the Technical Audit team can arrive on site to perform an audit of the agency's implementation. After conditional approval, you may proceed with a Smartphone or tablet implementation at the agency.

The New Audit

CJIS Security Policy 5.2 changes

- Visitor Logs
- Transaction Control Numbers exemption
- Smart Phones and Tablets
- Mobile Device Management
- Cloud Computing
- Next Version (5.3) changes
- New Audit Questions
- Future Policy discussions

Changes Under Consideration:

There are a number of things being discussed currently by the Security and Access Subcommittee and the APB regarding Policy changes.

These items are **NOT** current policy and are simply being discussed at this time. They may or may not show up in Policy in some future release (5.3/5.4/5.x?).

They are included here simply to make you aware of the discussions taking place.

Changes Under Consideration:

Changes to Policy being considered:

Putting all mobile (Laptops, Smart Phones, Tablets, other) into one new Policy area in the CSP – Section 5.13.

Task Force created by the FBI with reps from S+A, large, medium, and small agencies. (Two people from Texas)

Presented to S+A at the Fall 2013 meeting.

Changes Under Consideration:

Changes to Policy being considered

Allow an exemption for AA when the system with CJI on it has no direct connection to State or Federal repositories.

The CJI data has to be encrypted (not in a secure location).

Changes Under Consideration:

Changes to Policy being considered

Add language in the Policy that addresses the requirements for encrypting data at rest.

Set requirements for a passphrase to be used for the encryption.

Allow at-rest data to meet FIPS-197.

Changes Under Consideration:

Changes to Policy being considered

Add language in the Policy that addresses the requirements for PIN's.

Version 5.2 of the policy has a new best practice in Appendix G-5 that has things to consider when using PINs.

Under consideration to be moved into the main policy section as a requirement.

Questions/Contact Info:

Questions??????

Contact: Alan Ferretti
CJIS ISO – Texas
(512) 424-7186
alan.ferretti@dps.texas.gov

Web Site : www.dps.texas.gov/securityreview