Information Technology Security and the *CJIS Security Policy*

Nicholas Harris

CJIS Information Security Officer

Oregon State Police

Nicholas.harris@state.or.us

(503)302-7269

OBJECTIVE

- Why does OSP audit?
- What is the *CJIS Security Policy*?
- Where does the *CJIS Security Policy* come from?
- What is criminal justice information(CJI)?
- What to expect from an OSP IT audit?

OBJECTIVE

- What are the top noncompliance issues?
- Discussion of policy for top noncompliance issues

SHARED MANAGEMENT

- Where does CJI come from?
  - Local, state, tribal, and federal agencies
- Because the information is shared…
  - The FBI CJIS Division employs shared management philosophy

SHARED MANAGEMENT

- What does ‘shared management’ mean?
  - The FBI CJIS Division and its user community share responsibility for operation and management of shared information systems

SHARED MANAGEMENT

- How does ‘shared management’ work?
  - CJIS Systems Agency (CSA)
  - CJIS Systems Officer (CSO)
  - CJIS Information Security Officer (CISO)
  - CJIS Advisory Process
- The CJIS Advisory Process is used to…
  - Establish a minimum standard of requirements to ensure continuity of information protection

    (write minimum policy standards)

ADVISORY POLICY BOARD

- What does the Advisory Policy Board (APB) govern?
  - CJI obtained by criminal justice agencies for criminal justice purposes

COMPACT COUNCIL

- What does the National Crime Prevention and Privacy Compact Council (Council) govern?
  - CJI obtained by all agencies for noncriminal justice purposes

CJIS SECURITY POLICY

- Written by the user community (through the CJIS Advisory Process)
- Published yearly
- Current Version 5.6
- Provides minimum standard for IT security of CJI across the nation
- Over 600 ‘shall’ statements

CJIS SECURITY POLICY

- Where do the requirements come from?
  - Although the *CJIS Security Policy* is written by the user community in conjunction with the FBI through the Advisory Process, the requirements and language are often borrowed from the National Institute of Standards and Technology (NIST) [a part of the United States Department of Commerce]

CRIMINAL JUSTICE INFORMATION

- Definition:
  - 'Criminal Justice Information' is the term used to refer to all of the FBI CJIS Division provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data (i.e. any information obtained from the FBI)

CRIMINAL JUSTICE INFORMATION

- What does this mean?
  - CJI taken from FBI systems and copied, transposed, or scanned into local agency information systems (e.g. a records management system [RMS]) is still considered CJI and still falls under the scope of the *CJIS Security Policy*

CJIS AUDIT UNIT

- Why does OSP audit?
  - Formal audits are conducted to ensure compliance with applicable statutes, regulations and policies
  - Information housed in CJIS systems is obtained from the user community; the audit ensures that all agencies with access protect the data of the community at large

CJIS AUDIT UNIT

- Who does the OSP audit?
  - Each CJA and or NCJA every three (3) years
  - Vendors who have contractual CJIS with Oregon Agencies
- Who participates?
  - CJIS ISO visits the CJA/NCJA and small statistical sample of local agencies (number varies based on resources)
  - Looks for trends in the state

CJIS AUDIT UNIT

- What is the general audit process for the Agency
  - 4 to 6 weeks prior
    - Initial contact to local agency
    - Pre-audit material forwarded electronically

CJIS AUDIT UNIT

- What does the pre-audit material include?
  - Provides general idea of topic areas that will be discussed
  - List of documentation the agency is required to provide
  - Provides an idea of who to have present during the audit

CJIS AUDIT UNIT

- What happens the day of the audit?
  - Administrative Interview
  - Physical Security Inspection
    - Tour of the facility/datacenter
  - Policy Assessment Packet
    - Summarizes issues/concerns found

CJIS AUDIT UNIT

- What happens after the audit?
  - 60 days after (workload permitting)
    - Agency gets official draft report
  - 120 days after (workload permitting)
    - Response from Agency due

CJIS AUDIT UNIT

- What happens after the audit?
  - APB Compliance Evaluation Subcommittee (CES)
    - Criminal Justice
  - Compact Council Sanctions Committee
    - Noncriminal Justice
    - III misuse by Criminal Justice

NATIONAL AUDIT RESULTS

Criminal Justice Agencies
Event Logging
Encryption
System Use Notification
Advanced Authentication
Security Awareness Training
Management Control Agreements
Security Addendums
Media Disposal

NATIONAL AUDIT RESULTS

Noncriminal Justice Agencies
Contracted Noncriminal Justice Functions
Encryption
Event Logging
Personally Owned Computers
Mobile Devices
System Use Notification
Identification / User ID
Authentication (Passwords)

NATIONAL AUDIT RESULTS

CJA Top Findings	NCJA Top Findings
Personally Owned Computers	Contracted Noncriminal Justice Functions
Security Addendums	Personally Owned Computers
Encryption	Security Incident Response
Advanced Authentication	Security Awareness Training
Event Logging	Encryption
Security Incident Response	Physical Security
Management Control Agreements	Media Disposal
Media Protection	Mobile Devices
Security Awareness Training	Authentication (Passwords)

NATIONAL AUDIT RESULTS

Top Findings at both CJA and NCJA
Contractors (MCA/Security Addendum/Outsourcing)
Personally Owned Computers
Security Incident Response
Encryption
Security Awareness Training

FORMAL AGREEMENTS

- Before exchanging information…
  - Ensure a formal agreement is in place that specifies the terms of the relationship
    - Usage and dissemination restrictions
    - Access restrictions and training requirements
    - Physical and technical security controls for storage of information
    - Division of the roles and responsibilities
    - Security incident reporting procedures

FORMAL AGREEMENTS

Authorized Recipient	Performing Services	Type of Service	Agreement Needed
CJA	NCJA	Criminal Justice	Management Control Agreement
CJA	Private Contractor	Criminal Justice	Security Addendum
CJA	CJA	Criminal Justice	Information Exchange Agreement

FORMAL AGREEMENTS

- Management Control Agreement
  - Signed between the CJA agency head and the agency head of the noncriminal justice agency
- Applies only if ALL of the following are met:
  - ✓Using any outside noncriminal justice governmental agency
  - ✓To perform a criminal justice function
  - ✓With unescorted access to unencrypted CJI

FORMAL AGREEMENTS

- CJIS Security Addendum
  - Signed by each unescorted private contractor
  - Cannot be altered/substituted
- Applies only if ALL of the following are met:
  - ✓Using any outside personnel (not governmental)
  - ✓To perform a criminal justice function
  - ✓With unescorted access to unencrypted CJI

SCENARIO

The Sheriff's Office (a CJA) is receiving IT services from the County Department of Information Technology (a NCJA). IT services include desktop support and network administration. The information systems, containing CJI, are housed at the county IT data center with all other county government departments. All County IT personnel have unescorted access to the data center. The racks housing the Sheriff's Office equipment are not locked and the CJI is not encrypted at rest.

SCENARIO

Does the CJA need a management control agreement?

- ✓Using any outside noncriminal justice governmental agency
- ✓To perform a criminal justice function
- ✓With unescorted access to unencrypted CJI

SCENARIO

YES

SCENARIO

The Police Department (a CJA) is receiving custodial services from the City Facilities Department (a NCJA). Personnel are paid from Facilities budget and answer to the Director of City Facilities. All custodial personnel are allowed unescorted access to the Police Department, including secure terminal areas.

SCENARIO

Does the CJA need a management control agreement?

✓Using any outside noncriminal justice governmental agency

X To perform a criminal justice function

✓With unescorted access to unencrypted CJI

SCENARIO

NO

SCENARIO

The 911 Dispatch Center (a NCJA) provides MDTs for the Police Department (a CJA). The MDT application servers and networking are controlled and maintained by the 911 Center. The MDT laptops are issued and owned by the Police Department and are connected to the 911 via VPN connection.

SCENARIO

Does the CJA need a management control agreement?

- ✓Using any outside noncriminal justice governmental agency
- ✓To perform a criminal justice function
- ✓With unescorted access to unencrypted CJI

SCENARIO

YES

SCENARIO

The Sheriff's Office (a CJA) is using a local cloud storage company to store RMS backups containing CJI. The backups are encrypted at rest by the Sheriff's Office IT prior to leaving the facility and the Sheriff's Office manages the key infrastructure. The cloud vendor cannot unencrypt the data.

SCENARIO

Does the CJA need a signed CJIS Security Addendum?

✓Using any outside personnel (not governmental)

✓To perform a criminal justice function

X With unescorted access to unencrypted CJI

SCENARIO

NO

SCENARIO

The Police Department (a CJA) rents copiers from a private company. The copiers are being used by agency personnel to copy and/or scan CJI data. Every 2 years the copiers are replaced. The private company sends the CJA a certificate of destruction of all the hard drives.

SCENARIO

Does the CJA need a signed CJIS Security Addendum?

- ✓Using any outside personnel (not governmental)
- ✓To perform a criminal justice function
- ✓With unescorted access to unencrypted CJI

SCENARIO

YES

SCENARIO

City IT (a NCJA governmental) provides IT services and media destruction to a local Police Department (a CJA). City IT personnel have access to all of the Police Departments information systems containing CJI. The City IT has a subcontract with a local company for physical and electronic media destruction of all the city's media including the Police Department. Shredding is not witnessed by City IT.

SCENARIO

Does the CJA need a management control agreement?

- ✓Using any outside noncriminal justice governmental agency
- ✓To perform a criminal justice function
- ✓With unescorted access to unencrypted CJI

SCENARIO

YES

SCENARIO

Does the CJA need a signed CJIS Security Addendum?

- ✓Using any outside personnel (not governmental)
- ✓To perform a criminal justice function
- ✓With unescorted access to unencrypted CJI

SCENARIO

YES

PERSONNEL SECURITY

- Who needs a fingerprint-based record check for access to CJI?
  - All personnel with unescorted access to unencrypted CJI (whether access is physical or logical)

SCENARIO

The Sheriff's Office (a CJA) is receiving IT services from the County Department of Information Technology (a NCJA). IT services include desktop support and network administration. The information systems, containing CJI, are housed at the county IT data center with all other county government departments. All County IT personnel have unescorted access to the data center. The racks housing the Sheriff's Office equipment are not locked and the CJI is not encrypted at rest.

SCENARIO

Does the CJA need to submit fingerprints?

- ✓unescorted access to unencrypted CJI

SCENARIO

YES

SCENARIO

The Police Department (a CJA) is archiving all backup tapes with the City Archive Department (a NCJA). The tapes, containing CJI, are not encrypted at rest. A CJA employee takes the backup tapes to the Archive warehouse every Tuesday and locks the tapes within a CJA designated cage within the warehouse. State Archive personnel have key access to the cage for emergency purposes only but are supposed to request permission from the CJA prior to entry.

SCENARIO

Does the CJA need to submit fingerprints?

- ✓unescorted access to unencrypted CJI

SCENARIO

YES

SCENARIO

The Sheriff's Office (CJA) is using a well-known vendor for their mobile data terminal (MDT) direct access information system. The information system is administered by the vendor through remote maintenance (which is not initiated or monitored by the CJA). The private contractor has advised that they service many CJAs throughout the country and have been vetted in several other states.

SCENARIO

Does the CJA need to submit fingerprints?

- ✓unescorted access to unencrypted CJI

SCENARIO

YES

SECURITY AWARENESS TRAINING

- Who needs to complete security awareness training?
  - All personnel with unescorted access to unencrypted CJI (whether access is physical or logical)

SECURITY AWARENESS TRAINING

- When is security awareness training required?
  - Within 6 months of unescorted access
  - At least once every 2 years

SECURITY AWARENESS TRAINING

- What needs to be in the training?
  - **Level 1** – those with physical access only (not performing a criminal justice function – incidental access or "walking around access") [i.e. janitorial, maintenance, coke vendors, etc.]
  - **Level 2** – those with physical access only performing a criminal justice function (access on purpose) [i.e. paper shredding, records clerks, scanning services, couriers, etc.]

SECURITY AWARENESS TRAINING

- What needs to be in the training?
  - **Level 3** – those with physical and logical access (access to electronically see criminal justice info) [i.e. the majority of your staff, terminal operators, record entry, officer w/ mdts, etc.]
  - **Level 4** – those with IT

WRITTEN POLICY STANDARDS

- All important policy and procedures should be written for consistency and continuity of information…
  - Standards of discipline for misuse
  - Physical protection
  - Secure media storage, transport, and sanitization/disposal
  - Account management
  - Proper use/access from remote locations, using personal devices, mobile devices, etc.
  - Incident reporting

MEDIA PROTECTION

- Controlled access – at rest and in transit
- ID Verification and escort of visitor
- Secure sanitization/destruction
  - Authorized personnel
  - Witnessed
  - At least 3 passes for wipes

SYSTEM USE NOTIFICATION

- The system use notification shall provide the following:
  - The user is accessing a restricted information system
  - System usage may be monitored, recorded, and subject to audit
  - Unauthorized use of the system is prohibited and may be subject to criminal and/or civil penalties
  - Use of the system indicated consent to monitoring and recording

SYSTEM USE NOTIFICATION

- The system use notification must remain on the screen until user acknowledges the notification and takes explicit action to log in

IDENTIFICATION

- Each user shall be uniquely identified
  - No shared user accounts, no generic log in (especially includes remote maintenance by administrative IT personnel or private contractors)
- Least privilege
- Need–to–know

IDENTIFICATION

- Agency should have written policy and procedures for issuing user accounts as well as disabling and/or deleting of user accounts and performing validation of user accounts (annual audit of access)

AUTHENTICATION

- Passwords
  - Minimum of 8 characters
  - Numbers, letters, and special characters
  - Cannot be same as UserID
  - Expire in maximum of 90 days
  - Cannot reuse previous 10
  - Not transmitted in clear outside secure location

ADVANCED AUTHENTICATION

- What is two-factor authentication?
  1. Something you know (username and password)
  2. AND one of the following
     - Something you are (biometrics)
     - Something you have (token, one-time-password, etc.)

ADVANCED AUTHENTICATION

- When is advanced authentication (AA) required?
  - Direct access information systems accessed outside the physically secure location
  - This will affect the following:
    - User population
    - Remote maintenance to direct access system

ADVANCED AUTHENTICATION

- When is AA NOT required?
  - Access from within the physically secure location
  - Indirect access from outside the physically secure location

ADVANCED AUTHENTICATION

- Its important to note
  - Mobile devices that cannot support a full-featured operating system, may use compensating controls (e.g. mobile device management [MDM]) in lieu of AA as a temporary solution

ADVANCED AUTHENTICATION

- AA in the criminal justice conveyance
  - A criminal justice conveyance is considered a physically secure location and therefore, when officers are directly accessing CJI from within a criminal justice conveyance, AA is not required as long as the enclosed vehicle is meeting 5.9.1.3

ADVANCED AUTHENTICATION

- AA in the criminal justice conveyance
  - Mobile devices that cannot be removed or operate outside the criminal justice conveyance do not require AA
  - Conversely, mobile devices that can receive direct transactional responses from outside the criminal justice conveyance must implement AA
  - The APB did NOT approve written policy as a control to prevent use of an MDT outside the criminal justice conveyance as sufficient to meet the exemption

SCENARIO

A Police Department (a CJA) has mobile data terminals (MDTs) with direct access mounted within the police vehicle. The officers, by policy, remove the MDT from the vehicle each night and store within their home. The modem is in the trunk and the MDT cannot connect to the Police Department network to access CJI from outside the vehicle.

SCENARIO

Does the CJA need advanced authentication?

- ✓Direct access information system
- ✓Accessed from a physically secure location (criminal justice conveyance)
- ✓Will not work if removed from the secure location

SCENARIO

NO

SCENARIO

Here is why…

Although the officers have direct access to CJI, they cannot initiate a direct access transaction from outside the criminal justice conveyance, which is considered a physically secure location.

SCENARIO

A Police Department (a CJA) is using RMS software administered by private contractor. Private contractor personnel remote login at their leisure (session is not initiated by CJA) to the RMS server. The RMS is a direct access information system (i.e. can initiate transactions directly to the state /FBI). The CJA does not virtually escort contractors.

SCENARIO

Does the CJA need advanced authentication?

- ✓Direct access information system
- ✓Accessed from outside the physically secure location
- ✓Contractors can grant themselves direct access (as administrators)

SCENARIO

YES

SCENARIO

Here is why…

Because the private contractor personnel have remote access (access outside the physically secure location) to a direct access information system, they must utilize AA prior to accessing the direct access RMS.

Note: IT administrators, whether internal or external to the CJA, with elevated privileges pose a higher risk to CJI and the state/national network because of the nature of their knowledge and privileges within the network/system.

SCENARIO

The Police Department (a CJA) utilizes tablets (with a Windows 7 OS – full operating system) that have access to the agency's RMS. Although the RMS contains CJI, the system cannot perform transactional queries (run transactions).

SCENARIO

Does the CJA need advanced authentication?

- ✓Indirect access information system (cannot run transactions)

SCENARIO

NO

SCENARIO

Here is why…

Although CJA personnel have access to CJI through the RMS from outside a physically secure location, the RMS is an indirect information system and therefore does not require the implementation of AA.

ENCRYPTION

- When CJI is transmitted outside the boundary of the physically secure location, the data shall be immediately encrypted
  - Encryption for data in transit shall be a minimum of 128 bit and certified to meet FIPS 140-2 standards

ENCRYPTION

- When CJI is at rest (i.e. stored electronically) outside the boundary of the physically secure location, the data shall be encrypted
  - Encryption for data at rest can be a minimum of 256 bit and FIPS 197

SCENARIO

A Police Department (a CJA) has 4 precincts throughout the city which are connected by city owned fiber (city-wide WAN) to access their RMS system, which contains CJI. The city WAN is owned, operating, and maintained by the City IT Department, which has been authorized by the Police Department (thorough an MCA, fingerprints, and security awareness training).

SCENARIO

Does the CJA need encryption?

- ✓Contains CJI
- ✓Accessed/transmitted outside a physically secure location (from the RMS server location to 4 precincts throughout the city)

SCENARIO

YES

SCENARIO

Here is why…

Although the city owns, maintains, and operates the fiber connections transmitting CJI across the city, the CJA is unable to ensure physical access to the fiber is by authorized personnel only (fingerprinted, trained, etc.) for the entire length of the connection. Because the agency is unable to ensure all five conditions to meet the exemption, at least 128 bit FIPS 140-2 certified encryption must be employed between physically secure precincts.

ENCRYPTION

- Exception to encryption in transit only when…
  - Agency owns, operates, manages, or protects medium
  - Medium terminates within physically secure location on both ends, no interconnections
  - Physical access to the medium is controlled by the agency using the requirements of 5.9 and 5.12 (fingerprint-based record check)
  - Protection includes safeguards/countermeasures
  - Prior approval of the CSO

SCENARIO

The Sheriff's Office (a CJA) MDT server, a direct access information system, is located within the Sheriff's Office main building. The Sheriff's Office is using 'Local Teleco' provided aircards to connect laptops to the MDT server in order to run transactions in the criminal justice conveyance. The laptops are mounted and locked/secured in the physically secure criminal justice conveyance.

SCENARIO

Does the CJA need encryption?

- ✓Contains CJI
- ✓Accessed/transmitted outside a physically secure location (from the MDT server location to criminal justice conveyance)

SCENARIO

YES

SCENARIO

Here is why…

When CJI is transmitted outside the physically secure location (between the Sheriff's office and the criminal justice conveyance), at least 128 bit FIPS 140-2 encryption must be employed.

SCENARIO

The Police Department (a CJA) using a private contractor to service their MDT application, a direct access information system. The MDT server is located within the Police Department. Private contractor personnel have remote access to the server, and CJI, using a virtual private network (VPN).

SCENARIO

Does the CJA need encryption in transit?

- ✓Contains CJI
- ✓Accessed from outside a physically secure location (remote access from anywhere)

SCENARIO

YES

SCENARIO

Here is why…

When CJI is accessed outside the physically secure location (between the Police Department where the server is and the contractors laptop), at least 128 bit FIPS 140-2 encryption must be employed.

SCENARIO

A Police Department (a CJA) is using a cloud vendor to store their backups of their RMS data, containing CJI. Backups of the data are encrypted by the Police Department using at least 256 bit FIPS 197 encryption prior to being sent via the internet to the cloud vendor's facility in a neighboring state.

SCENARIO

Does the CJA need encryption in transit?

- ✓Contains CJI
- ✓Transmitted outside a physically secure location (from the agency to cloud)

SCENARIO

YES

SCENARIO

Here is why…

Although the 256 bit FIPS 197 encryption can be used for the data at rest in the cloud vendor's facility (a non-secure location), because the information is sent via the internet (outside the secure location of the Police Department) the standard must be at least 128 bit FIPS 140-2 certified encryption. The agency can either encrypt the data at rest to the higher FIPS 140-2 standard or send the information as is (197) using FIPS 140-2 encryption on the connection method (e.g. VPN).

SCENARIO

The Police Department (a CJA) has a disaster recovery (DR) site that is managed by the city IT Department (a NCJA) [which has been authorized through an MCA, fingerprint checks, and training]. Backups of the information system, containing CJI, are replicated using a virtual storage area network (SAN) from the PD to the DR [SAN to SAN]. The CJA is not encrypting the data at rest prior to transit.

SCENARIO

Does the CJA need encryption in transit?

- ✓Contains CJI
- ✓Transmitted outside a physically secure location (from the agency to DR)

SCENARIO

YES

SCENARIO

Here is why…

When CJI is transmitted outside the physically secure location (between the PD and DR location), at least 128 bit FIPS 140-2 encryption must be employed.

Note: Proprietary segmentation of the data prior to transit is not equivalent to encryption and does not exempt the agency from encryption requirements.

EVENT LOGGING

- If a security related event took place (i.e. a breach of your information)…
  - Who did it
  - When it happened
  - What happened

EVENT LOGGING

- Log content
- Weekly review of audit logs
- Retain for minimum of 365 days

MOBILE DEVICES

- Limited featured operating systems cannot support certain IT security controls
- Mobile device management (MDM)
- Unique concerns for usage restrictions and implementation guidelines

CLOUD COMPUTING

- Physical and logical access control
- Metadata/data mining/analytics
- Data recovery/sanitization

CONTACT INFORMATION

Nicholas Harris

CJIS Information Security Officer

(503) 302-7269

<Nicholas.harris@state.or.us>