Information Technology

Security Awareness Training for Administrative Personnel

This training information is intended for criminal justice Administrative Personnel without direct access to IDACS/CJIS systems.

Other training is available for Operators and Information Technology Professionals.

IT Security Awareness Training

This training implements a requirement of the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division’s CJIS Security Policy Version 5.0 that all personnel who have access to criminal justice information receive security awareness training within six months of initial assignment, and biennially thereafter.

Information System

To understand the importance of information system security or information technology security, you first need to know what an information system is.

Information System

The term "**information system**" means:

- ❖ a unique set of information resources …
- ❖ organized …
- ❖ for the …
  - collection,
  - processing,
  - maintenance,
  - use,
  - sharing,
  - dissemination, or
  - disposition …

… of information, in this case

"**Criminal Justice Information**" **(CJI)**

Information System

An information system may also include other communications equipment, such as …

- Mobile Data Terminals,
- laptops, tablet computers, iPads
- handheld computers,
- smart phones (BlackBerry, Android phones),
- printers,
- fax machines,

etc …

Information Technology Security

The term "**information security**" refers to protection of information and Information Technology (IT) systems from unauthorized:

- access,
- use,
- disclosure,
- disruption,
- modification, or
- destruction …

… in order to provide:

- Confidentiality
- Integrity
- Availability
- Authenticity
- Non-Repudiation

Confidentiality

… means that information is not disclosed to unauthorized individuals.

… ensures that access to information and services is restricted to those with the need-to-know, using the principle of least necessary privilege.

Integrity

… means assurance that information and systems are not modified maliciously or accidentally.

… ensures that information is reliable, accurate, and under organizational control. This means that users must be identified to prevent unauthorized modifications.

Availability

… means reliability of timely access to data and resources by authorized individuals.

… ensures that the system is up and running when a user needs to access it.

Authenticity

… means confidence that information actually comes from the source that it claims to be from.

… ensures that a person or system requesting access is who or what they claim to be, by requiring information that only the **authentic** entity would know or possess.

Non-Repudiation

… means preventing a user from denying an action by securely logging all information activity.

… ensures that every action taken in the system can be traced back to the actual person that performed the action.

Why is IT Security Important?

- Government/businesses/individuals increasingly depend on information technology systems. Protecting these assets is more important than ever before.

- Systems have become increasingly more complex and interconnected, making them more difficult to secure and increasing risk.

Why is IT Security Important?

Bottom line …

FBI/CJIS Requirement.

Online Security Versus Online Safety

Security: We must secure our computers with technology in the same way that we secure the doors to our offices.

Safety: We must act in ways that protect us against the risks and threats that come with Internet use.

What is “Security Awareness”

- **Security awareness** is the knowledge and attitude members of an organization possess regarding the protection of the physical and, especially, information assets of that organization.

What is “Security Awareness”

- ❖ Being security aware means you understand that there is the potential for some people to deliberately or accidentally steal, damage, or misuse the data that is stored within an organization’s company's computer systems.

What is "Security Awareness"

- Being security aware guards the information property of the organization by trying to stop attacks from happening. To stop attacks from happening, you must be "aware" of:
  - What information you have access to;
  - How an attacker might try to gain access to it;
  - What **YOU** can do to block an attacker's access.

Security Awareness Training

Required:

- Within six months of assignment, and
- Every two years thereafter.

Security Awareness Training

Required:

- For all personnel who have access to criminal justice information (CJI), including:
  - New employees
  - Current users
  - Personnel who manage users
  - IT personnel
  - Contractors
  - Personnel with physical access
    - Custodial
    - Administrative
      - Department Heads
      - Secretarial

Security Awareness Training

Required:

- For new operators
  - Separate test & certification in nexTEST
  - Certification required prior to class

Security Awareness Training

Required:

- ❖ For existing operators
  - Security Awareness Training built in to standard operator/coordinator certification & test in nexTEST
  - Follow regular recertification schedule

Security Awareness Training

Required:

- For non-operators (administrative staff, non-criminal justice agency staff, contractors)
  - Review slides
  - Sign affirmation of review (a document stating when and where you viewed Security Awareness Training.)

Security Training Records

- Document
- Keep Current
- Maintain for Audit

Security Training Records

An agency may accept documentation of training from another agency. HOWEVER, accepting such training documentation from another agency means assuming the risk that the training may not be adequate to meet federal or state requirements.

Security Awareness Topics

All Personnel

- ❑ Rules and responsibilities
- ❑ Disciplinary consequences
- ❑ Incident response
- ❑ Threats, vulnerabilities, and risks
- ❑ Visitor control and physical security
- ❑ Protect confidentiality concerns
- ❑ Protecting “media”
- ❑ Proper handling and marking
- ❑ Dissemination and destruction

Security Awareness Topics

Personnel with Electronic Access (Operators)

- ❑ Individual accountability
- ❑ Password management
- ❑ Social engineering
- ❑ Phishing
- ❑ Unknown e-mail / attachments
- ❑ Spam
- ❑ Protection from malware
- ❑ Web usage
- ❑ Publicly accessible computers
- ❑ Personally-owned equipment
- ❑ Desktop security
- ❑ Notebook security
- ❑ Handheld device security
- ❑ Access control
- ❑ Encryption

Security Awareness Topics

Personnel with Information Technology Roles

- ❑ Access control measures
  - ❑ Access control mechanisms
  - ❑ 802.11 Wireless access restrictions
- ❑ Protection from malware
  - ❑ Scanning
  - ❑ Updating definitions
- ❑ Configuration management
  - ❑ Network Diagrams
  - ❑ Timely application of system patches
- ❑ Data backup and storage
- ❑ Electronic sanitization
- ❑ Network infrastructure protection

Security Awareness Topics

FOR ALL PERSONNEL

CJIS Security Policy

The CJIS Security Policy, established by the CJIS Advisory Policy Board (APB) and approved by the Director of the FBI, provides the minimum level of security requirements determined acceptable for the transmission, processing, and storage of Criminal Justice Information (CJI).

They include:

- Rules of behavior policy for CJI users
- Laws, regulations and management goals
- Security Procedures

CJIS Security Policy

- Integrates:
  - Presidential directives
  - Federal laws
  - FBI directives
  - Criminal justice community APB decisions
  - National Institute of Standards and Technology guidance

to provide controls to protect the full lifecycle of CJI, whether it is being communicated (in transit) or being stored (at rest).

CJIS Security Policy

- Provides guidance for CJI:
  - Creation
  - Viewing
  - Modification
  - Transmission
  - Dissemination
  - Storage
  - Destruction

CJIS Security Policy

- Applies to every individual –
  - Contractor,
  - Private entity,
  - Noncriminal justice agency representative, or
  - Member of a criminal justice entity

– with access to, or who operate in support of, criminal justice services and information.

CJIS Security Policy

- Establishes the **minimum protection** requirements that must be implemented for all CJI systems.
- Individual agencies and the control agency:
  - Indiana State Police/IDACS Committee
  - Regional dispatch centers
  - Local law enforcement

  may implement **more stringent protection** measures than the CJIS Security Policy.

Standards of Discipline

Criminal Justice Information (CJI) is

Sensitive Information

CJI includes:

- ❖ Criminal History Record Information (CHRI)
- ❖ Personally Indentifying Information (PII)
- ❖ Investigative Information

Improper access, use, or dissemination of CJI is serious!

Standards of Discipline

Improper access, use, or dissemination of CJI may result in:

- Sanctions against your agency, including:
  - Notice of Violation
  - Notice of Probation
  - Suspension of services
  - Termination of services

Action may be taken **both** against your agency and ***AGAINST YOU*** personally.

Standards of Discipline

Improper access, use, or dissemination of CJI may result in:

- Sanctions ***AGAINST YOU***, including:
  - Suspension of system access
  - Termination of employment
  - Civil penalties up to $11,000
  - Federal and/or state criminal penalties

Action may be taken ***AGAINST YOU*** by the local agency, the control agency, the FBI, or all three.

CJIS Systems Agency

The **CJIS Systems Agency (CSA)** is the duly authorized state, federal, international, tribal, or territorial criminal justice agency on the CJIS network providing statewide (or equivalent) service to its criminal justice users, with respect to the CJIS data from various systems managed by the FBI CJIS Division.

There is only one CSA per state or territory.

The **Indiana State Police (ISP)** serves as the **CSA** for all criminal justice agencies in Indiana.

CJIS Systems Agency

The CSA is responsible for:

- Establishing and administering the CJIS IT Security Program, and
- Enforcing system security and discipline throughout the CJIS user community, down to and including local agencies.

The CSA may impose **more stringent protection** measures than the CJIS Security Policy requires.

CJIS Systems Officer

The **CJIS Systems Officer (CSO)** is an individual responsible for the administration of the CJIS network for the CSA.

- The CSO must be an employee of the CSA.
- The role of the CSO may not be outsourced.
- The Chairman of the IDACS Committee,

  ISP Lt. Col. John W. Clawson,

  serves as the **CSO** for the State of Indiana.

CJIS Systems Officer

The CSO is responsible for:

- Setting
- Maintaining
- Enforcing

policies that govern the operations of:

- Computers
- Access devices
- Networks
- and other components that comprise and support

CJIS systems that process, store, or transmit criminal justice information within the CSA's jurisdiction.

CJIS Systems Officer

The CSO is responsible for:

- Setting
- Maintaining
- Enforcing

statewide standards for the:

- Selection
- Supervision
- Separation

of personnel who have access to criminal justice information and systems within the CSA’s jurisdiction.

CJIS Systems Officer

The CSO is responsible for:

- Ensuring:
  - Appropriate use of all CJI systems and services.
  - CJIS operating procedures are followed by all users.
  - Agency compliance with the policies approved by the CJIS Advisory Policy Board and adopted by the FBI.
  - Terminal Agency Coordinator is designated for every agency with devices accessing CJI systems or information.
  - Local Agency Security Officer (LASO) is designated for every agency with access to CJI information.
    - Usually, the Terminal Agency Coordinator (TAC) serves as the LASO.

CJIS Systems Officer

The CSO is responsible for:

- Approving access to FBI CJIS systems.
  - Reviewing terminal and non-terminal agency applications
  - Reviewing terminal operator requests
- Appointing a CSA Information Security Officer (CSA ISO) for the state.
- Enforcing system discipline.
- Ultimately managing the security of CJIS systems within their state or agency.

CSA Information Security Officer

The **CSA Information Security Officer (CSA ISO)** is an individual appointed by the CSO with delegated authority to administer the CJIS Information Security Program.

The CSA ISO is responsible for:

- Serving as Point-of-Contact for the CJIS ISO.
- Documenting technical compliance with the CJIS Security Policy, including at the local level.
- Assisting agencies with implementing controls in accordance with CJIS Security Policy.

CSA Information Security Officer

The CSA ISO is responsible for:

- Establishing a security incident response and reporting procedure to:
  - Discover,
  - Investigate,
  - Document, and
  - Report

  major incidents that significantly endanger the security or integrity of the criminal justice agency systems.

CSA Information Security Officer

The CSA ISO is responsible for:

- Reporting security incidents to:
  - the CSA,
  - the affected criminal justice agency, and
  - the FBI CJIS Division ISO

Local Agency Security Officer

The **Local Agency Security Officer (LASO)** is an individual appointed by the local agency head to administer the CJIS Information Security Program.

The LASO is responsible for:

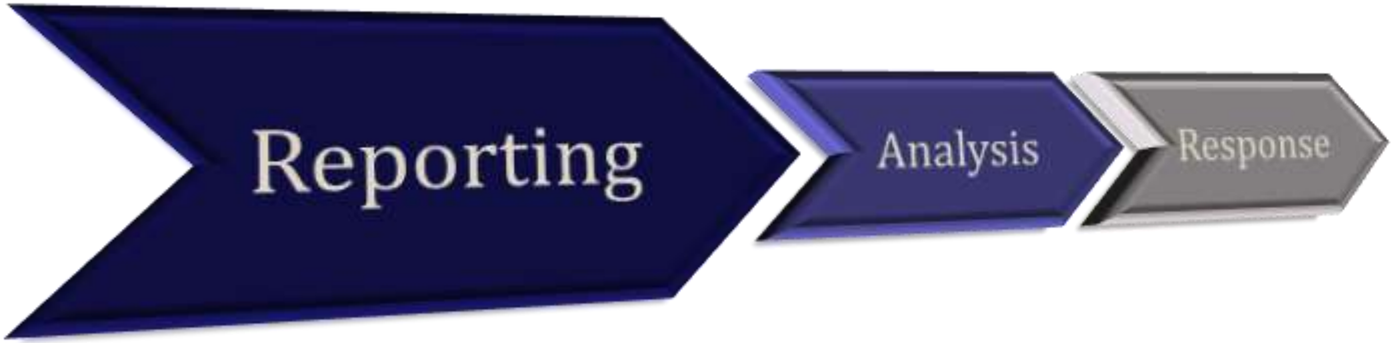
- Serving as Point-of-Contact for the CSA ISO.
- Ensuring approved and appropriate security measures are in place and working as expected.
- Supporting compliance with CJIS and CSA security policy in cooperation with the CSA ISO.
- Ensuring security incidents are promptly reported to the CSA ISO.

Local Agency Security Officer

The LASO is responsible for:

- Identifying who is using approved hardware, software, and firmware to access CJIS systems.
- Ensuring against unauthorized access to CJIS systems.
- Identifying and documenting how local agency equipment connects to the CSA system, including:
  - Network diagrams
  - Equipment inventory
  - IP addresses

Security Incident Reporting



Reporting

Analysis

Response

Security Incident Reporting

Report each security incident:

- Terminal agency name & ORI
- LASO contact information
- Incident date & time
- Incident location
- Source/destination IP address, port, & protocol
- Operating system version, patches, etc.
- Antivirus software version
- Impact to agency
- US-CERT Category (*see next slide*)

Security Incident Reporting

Category	Name	Description	Reporting time
CAT 0	Exercise/Network Defense Testing	Testing internal / external defenses or responses.	N/A; this category for local agency internal use only
CAT 1	*Unauthorized Access	Active hacking, network penetration	Within one (1) hour of discovery
CAT 2	*Denial of Service (DoS)	Flooding of the network, exhausting resources	Within two (2) hours of discovery
CAT 3	*Malicious Code	Trojan horse, virus, worm, other malicious code-based attack	Daily, or within one (1) hour of wide-spread discovery
CAT 4	*Improper Usage	Violation of policy	Weekly
CAT 5	Scans, Probes, Attempted Access	No direct compromise or denial of service	Within one (1) hour of discovery
CAT 6	Investigation	Unconfirmed incidents warranting review	N/A; local agency internal use only

Security Incident Reporting

Report each security incident to:

ISP IDACS Section <IISP@isp.IN.gov>

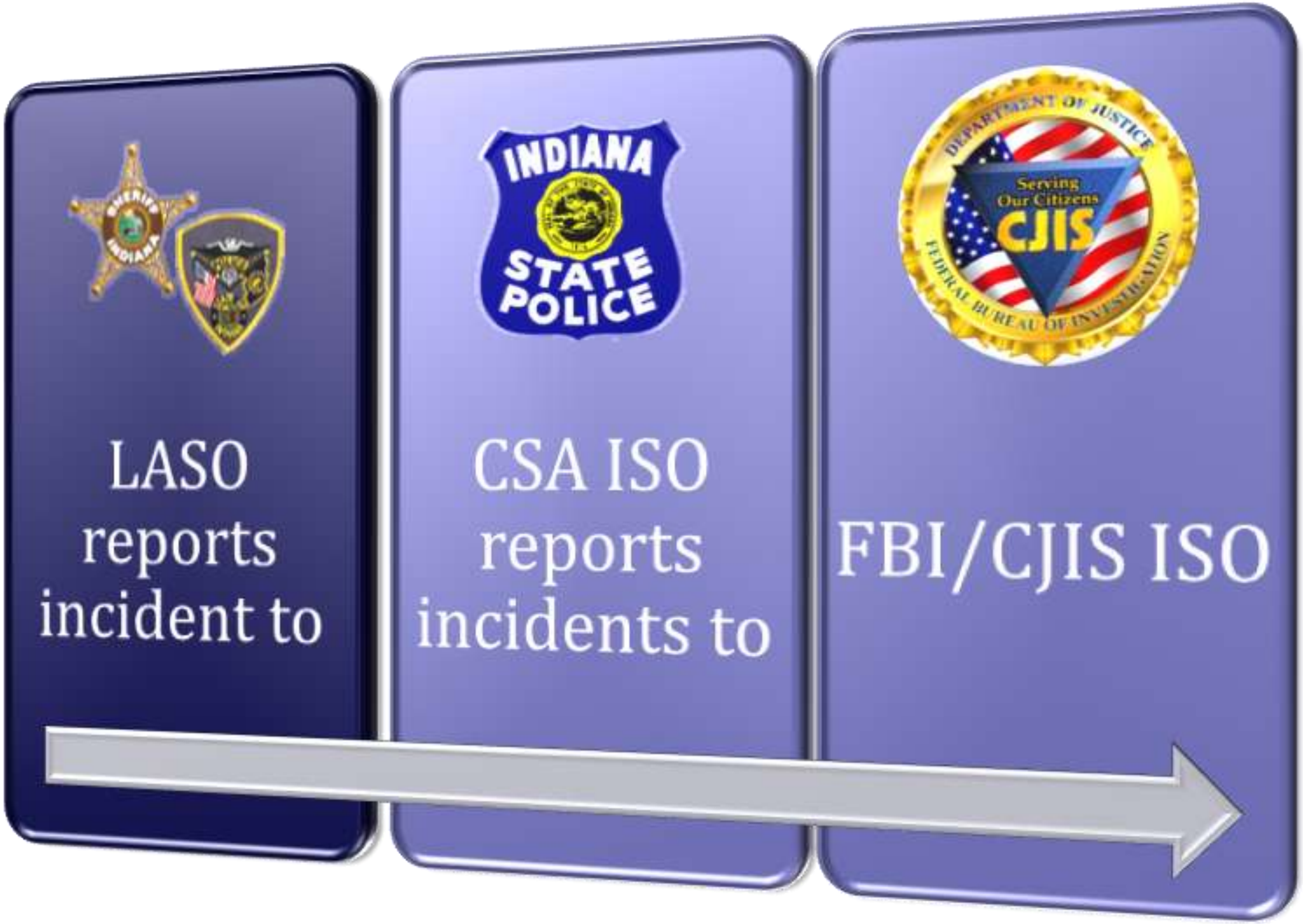
ATTN: Information Security Officer

Subject: COMPUTER SECURITY INCIDENT:
[Your Agency ORI] – [Your Agency Name]

Or send a switched message to:

INISP0000 – ISP Data Operations Center

Security Incident Reporting



LASO reports incident to

CSA ISO reports incidents to

FBI/CJIS ISO

Vulnerabilities and Threats

Vulnerability

- A point where a system is susceptible to attack.
- Vulnerabilities may include:
  - Physical
  - Natural
  - Media
  - Human
  - Communication
  - Hardware and Software

Vulnerabilities and Threats

Threat

- An unintentional or deliberate event or circumstance which could have an adverse impact on an information system.
- Can come from internal or external sources.
- There are three main categories of threats:
  - Natural
  - Unintentional
  - Intentional

Vulnerabilities and Threats

Natural threats

- Can endanger any facility or equipment.
- Usually not preventable.
- Natural threats include:
  - Fire
  - Flood
  - Lightning
  - Power Failures
- ***Damage can be minimized with proper planning.***

Vulnerabilities and Threats

Unintentional threats

- Actions that occur due to lack of knowledge or through carelessness.
- Can be prevented through awareness and training.
- Unintentional threats include:
  - Physical damage to equipment
  - Deleting information
  - Permitting unauthorized users to access information

Vulnerabilities and Threats

Intentional threats

- Deliberately designed to harm or manipulate an information system, its software or data.
- Often conducted by “insiders”.
- Security software such as an antivirus program is designed to protect against intentional threats.
- Personnel security measures help mitigate the possibility of “insider threats”.

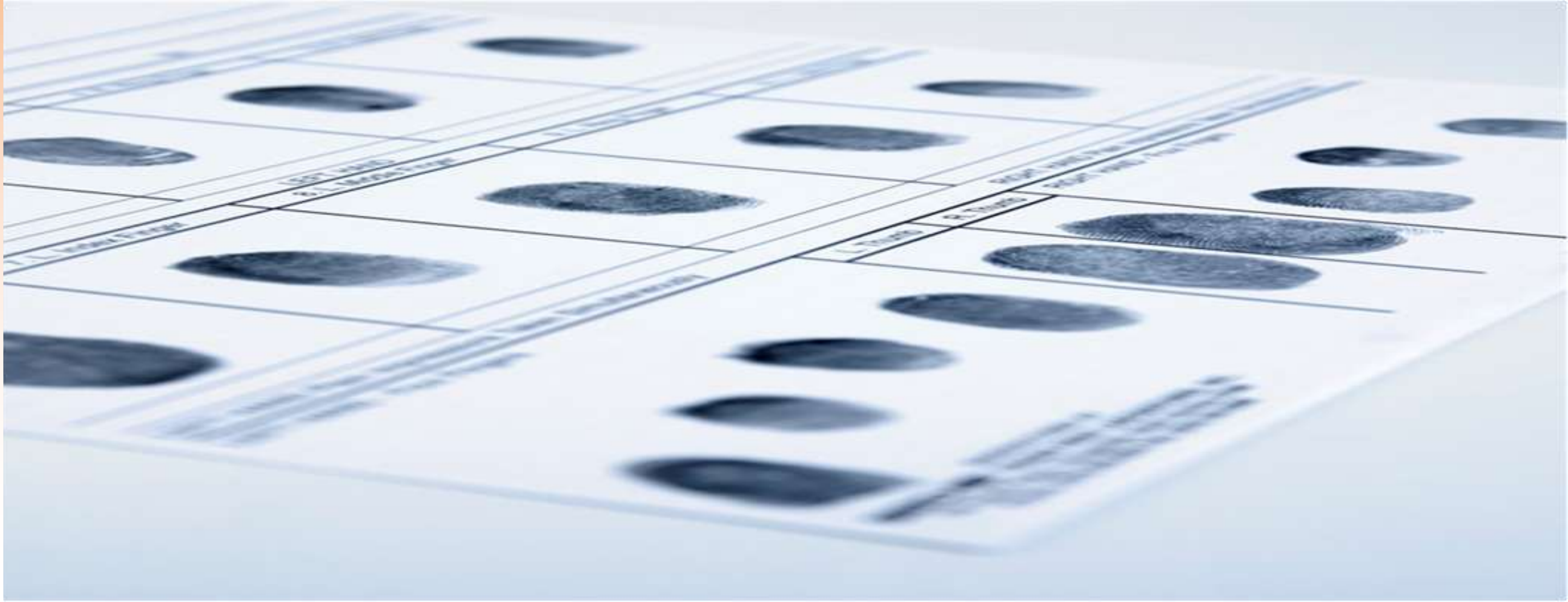
Vulnerabilities and Threats

Intentional threats

- Intentional threats include:
  - Intrusions
  - Denial of Service
  - Unauthorized access to data or systems
  - Theft
    - Physical device theft
    - Electronic theft
      - Identity Data
      - Electronic Funds
  - Sabotage
  - Eavesdropping
  - Social Engineering
  - Phishing

Personnel Security

Protects against “insider threat” by reducing the likelihood of untrustworthy personnel gaining access to the system.



Personnel Security

- **Fingerprint-based record check**
  - State of residency (CHRIS) + national (III)
  - Within 30 days of employment or assignment.
  - Felony conviction = **NO ACCESS**
  - CSO review required for:
    - Any other conviction
    - Arrest without conviction
    - Apparent fugitive (NCIC/Canadian/INTERPOL want)
    - Subsequent arrest or conviction after CJI access
    - Moral turpitude

Personnel Security

- **Fingerprint-based record check**
  - Required for individuals:
    - With direct access to CJI
    - Responsible for CJI systems and networks
    - Unescorted personnel with access to physically secure areas:
      - Support personnel
      - Contractors
      - Custodial workers
  - **Re-investigation every five (5) years**

Personnel Security

Termination of Employment

- Terminate all local access immediately
  - Physical access
  - Computer accounts
- Notify CSA to terminate system access
  - IDACS
  - nexTEST

Personnel Security

❖ Reassignment / Transfer

- Terminate *unneeded* local access
  - Physical access
  - Computer accounts
- ***Change*** system access to *appropriate* levels
  - IDACS (i.e. change “Full Operator” to “Inquiry Only”)
  - nexTEST
  - Local accounts

Personnel Security

❖ Personnel Sanctions

- Formal process required at local agency level
- Policy must be written and distributed

Physical Security

Physically Secure Location

- Facility, area, room, or group of rooms, or
- Police vehicles until September 30th, 2013
- Subject to:
  - Criminal justice agency management control;
  - SIB control;
  - FBI CJIS Security addendum;
  - or a combination thereof
- With both
  - Physical security controls, and
  - Personnel security controls.

Physical Security

Physically Secure Location

- Security Perimeter
  - Prominently posted
  - Separated from non-secure locations
- Physical Access Authorization
  - Know and document who is authorized
  - Issue credentials
- Physical Access Control
  - Control access points
  - Verify access authorizations

Physical Security

Physically Secure Location

- Control access to communication lines
  - Includes inside closets and outside access points
  - Identify all outside communication repair persons
- Control access to display devices
  - Keep screens turned away from visitors
  - Install screen filters
- Monitoring Physical Access
- Respond to physical security incidents

Visitor Control

- Authenticate visitors before granting access

- Escort visitors at all times

- Monitor visitor activity

Visitor Control

- Log all visitors – maintain logs one year
  - Name and agency of the visitor
  - Form of identification
  - Date of access
  - Time of entry and departure
  - Purpose of visit
  - Name and agency of person visited
  - Signature of the visitor
- Review logs frequently for completeness

Sensitive Information Use

Criminal History Record Information (CHRI)

- Collected by criminal justice agencies
- on individuals
- consisting of identifiable descriptions of:
  - Arrests
  - Detentions
  - Indictments
  - Informations
  - Other formal criminal charges
  - Dispositions, including
    - Acquittal
    - Sentencing
    - Correctional supervision
    - Release

Sensitive Information Use

❖ Criminal History Record Information (CHRI)

- Access only for authorized purpose (PUR/):
  - C – Criminal Justice (other than employment)
  - D – Domestic Violence and Stalking (Courts only)
  - F – Weapons-Related Background Checks
  - H – Housing (Public Housing Authorities only)
  - J – Criminal Justice Employment (incl. vendors)
  - X – Exigent Procedures (e.g. child placement)
- **Use only for purpose accessed!**

Sensitive Information Use

Criminal History Record Information (CHRI)

- May be disseminated to another (i.e. "non-terminal") agency if either:
  - The other ("non-terminal") agency is
    - **authorized to receive** CHRI, and
    - is being serviced by the accessing ("terminal") agency

  OR

  - The other agency is performing personnel and appointment functions for criminal justice employment applicants (i.e. a centralized HR agency).

Sensitive Information Use

NCIC Restricted Files Information (RFI)

- Restricted Files include:
  - Gang Group and Gang Member Files
  - Known or Appropriately Suspected Terrorist File
  - Convicted Persons on Supervised Release File
  - Immigration Violator File
  - National Sex Offender Registry File
  - Protection Order File (Cleared/Expired Orders only)
  - Identity Theft File
  - Protective Interest File
  - Missing Person File Person with Information [PWI] data

Sensitive Information Use

NCIC Restricted Files Information (RFI)

- Access, use, and dissemination consistent with CHRI.
- No purpose codes used; but purpose must be logged when accessed;
  - Who requested (unique identifier, i.e. badge number)
  - Why requested (criminal case; criminal justice employment background; hit from traffic stop, etc.)
  - Case or CAD Number
- **Use only for purpose accessed!**

Sensitive Information Use

NCIC Non-Restricted Files Information (NFI)

- Non-Restricted Files include:
  - Stolen Articles
  - Stolen Boats
  - Foreign Fugitives
  - Stolen and Unreported Recovered Guns
  - Stolen License Plates
  - Missing Persons (other than PWI data)
  - Stolen Securities
  - Stolen Vehicles
  - Stolen Vehicle and Boat Parts
  - Wanted Persons
  - Unidentified Persons and Body Parts

Sensitive Information Use

- **NCIC Non-Restricted Files Information (NFI)**
  - Access and use for any ***authorized*** purpose
  - May be disseminated to
    - Other government agencies
    - Private entities authorized by law

  at the discretion of the CSO

Sensitive Information Use

NCIC Non-Restricted Files Information (NFI)

- Bulk data requests discouraged
- Access for non-law enforcement purposes is only permitted to confirm status of property or person (i.e. “wanted” or “stolen”, etc.)
  - Access only by authorized criminal justice personnel
  - No details may be provided
  - Nominal administrative fee may be charged
- Commercial dissemination **PROHIBITED**

Sensitive Information Use

Personally Identifiable Information (PII)

- Information which can be used to distinguish or trace an individual's identity
  - Name
  - SSN
  - Photograph
  - Biometrics
    - Fingerprints
    - Hand
    - Face
    - Voice
    - Retina
    - Iris
    - DNA
- Alone or combined with other personal or identifying information, such as
  - Date of birth
  - Mother's maiden name

Sensitive Information Use

- **Personally Identifiable Information (PII)**
  - Extracted **F**or **O**fficial **U**se **O**nly (**FOUO**)
  - Use appropriate controls to safeguard
  - Auditing, logging, other security beyond the scope of this policy
  - **Use only for purpose accessed!**

Storing Sensitive Data

- Today's crime scene is in your:
  - Workplace
  - Home office
  - Living room

Storing Sensitive Data

Sensitive Data

- Criminal History Record Information (CHRI)
- Personally Identifiable Information (PII)
- Store only when key to criminal or case files
- Establish appropriate safeguards
  - Administrative
  - Technical
  - Physical
- Ensure security and confidentiality

Protecting Media

- “Media” includes:
  - Hard disk drives
    - External
    - Internal
      - Workstations
      - Notebooks
      - Office printers (!)
  - Floppy disks
  - USB “flash” drives
  - Memory cards
  - Smart phones
  - Handheld (PDA) computers
  - CD/DVD
  - Tapes
  - Printouts
  - Photographs

Protecting Media

- Store media securely
  - Physically secure location
  - Access restricted to authorized personnel
- Transport media securely
  - Maintain physical control
  - Restrict transport activities to authorized personnel
- Encrypt electronic media
  - In storage
  - In transit

Proper Handling and Marking

- Handling
  - Protect the media against unauthorized:
    - Disclosure
    - Alteration
    - Misuse

Proper Handling and Marking

- Handling
  - Know who you give it to:
    - Deliver it personally.
    - Confirm recipient’s identity.
    - Verify recipient’s purpose.
    - Log every dissemination.

Proper Handling and Marking

- Marking
  - Know what information is in your hands.
    - Four main categories of information:
      - Criminal History Record Information (CHRI)
      - NCIC Restricted Files Information (RFI)
      - NCIC Non-Restricted Files Information (NFI)
      - Personally Identifiable Information (PII)
  - Label it clearly so as not to mistake its importance.

Disposal of Media

- Electronic sanitization:
  - Overwrite at least three times
    - Use secure “disk wipe” software utilities
    - Good standards to look for in a utility:
      - US Army AR380-19
      - US Air Force 5020
      - US Department of Defense DoD 5220.22-M (E)
      - US Department of Defense DoD 5220.22-M(ECE)
  - Alternatively, degauss (demagnetize) media
    - Permanently destroys usability
  - Physically destroy when no longer needed

Disposal of Media

Physical disposal:

- ❖ Shred

or

- ❖ Burn

Disposal of Media

Physical disposal:

- Ensure destruction or disposal is either
  - Carried out, or
  - Witnessed

by authorized personnel

Disposal of Media

DO NOT PLACE SENSITIVE DATA IN TRASH CANS!

CJIS Audits

- CJIS Audit Unit will conduct a compliance audit every three years of each CSA.
- The CSA will conduct audits on all criminal justice and noncriminal justice agencies every three years.

CJIS Audits

- All system transactions are subject to review for inappropriate or illegal activity.

- The purpose of the audit is to ensure compliance with agency and FBI CJIS Division policy and regulations.

Report Security Violations

If you become aware of any policy violation, or suspect that your password may have been used by someone else, it is your responsibility to report that information immediately to your respective Security Officer.

Remember

- It’s your responsibility to ensure you’re aware of and adhere to all policies and procedures regarding IT Security

- If you have any questions about the proper operation or security of computer systems entrusted to you, contact your Security Officer

What is the weakest link to having a successful Security Program?

The key to security begins with **YOU**

Congratulations!

You have successfully completed Indiana’s CJIS Security Awareness Training.

Please print and fill out the next page, and submit it to your Local Agency Security Officer.

IDACS/CJIS Security Awareness Certification for Administrative Personnel

- I, ______________________________
  (printed name)
  hereby certify that I have thoroughly reviewed and do understand the concepts presented in the IDACS/CJIS Security Awareness Training materials.
- I acknowledge that I will be held accountable to properly apply this knowledge in any and every circumstance in which I am handling, exposed to, or otherwise have access to criminal justice information likely obtained from any Indiana State Police criminal justice information system.

______________________________ ______________

Signature Date

______________________ ______________________

Title Organization

Agency Security Officer Acknowledgement:

______________________________ ______________

Agency Security Officer's Signature Date

______________________ ______________________

Title Criminal Justice Agency