Information Technology

Security Awareness Training for Operators

This training information is intended for criminal justice OPERATORS with *direct access* (via a User ID) to IDACS/CJIS systems.

Other training is available for Administrative Personnel 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.

Security Awareness Training

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.

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

Information Technology Security

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.

Information Technology Security

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?

Bottom line …

FBI/CJIS Requirement.

Security Awareness Training

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.

Security Awareness Training

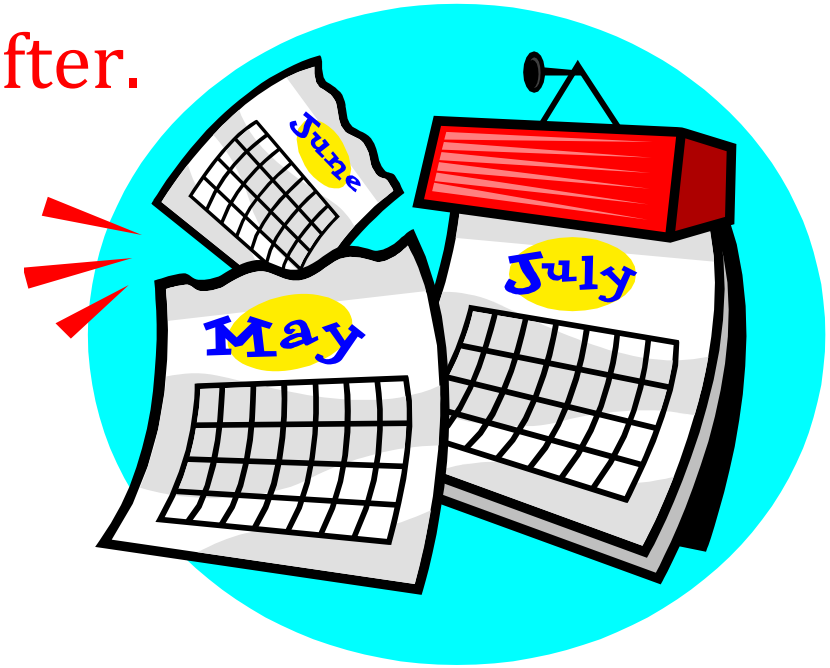
What is "Security Awareness"

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

Security Awareness Training

Required:

- For existing operators
  - Security Awareness Training will follow a standard operator/coordinator certification schedule and test in nexTEST.

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

- 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

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

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”.

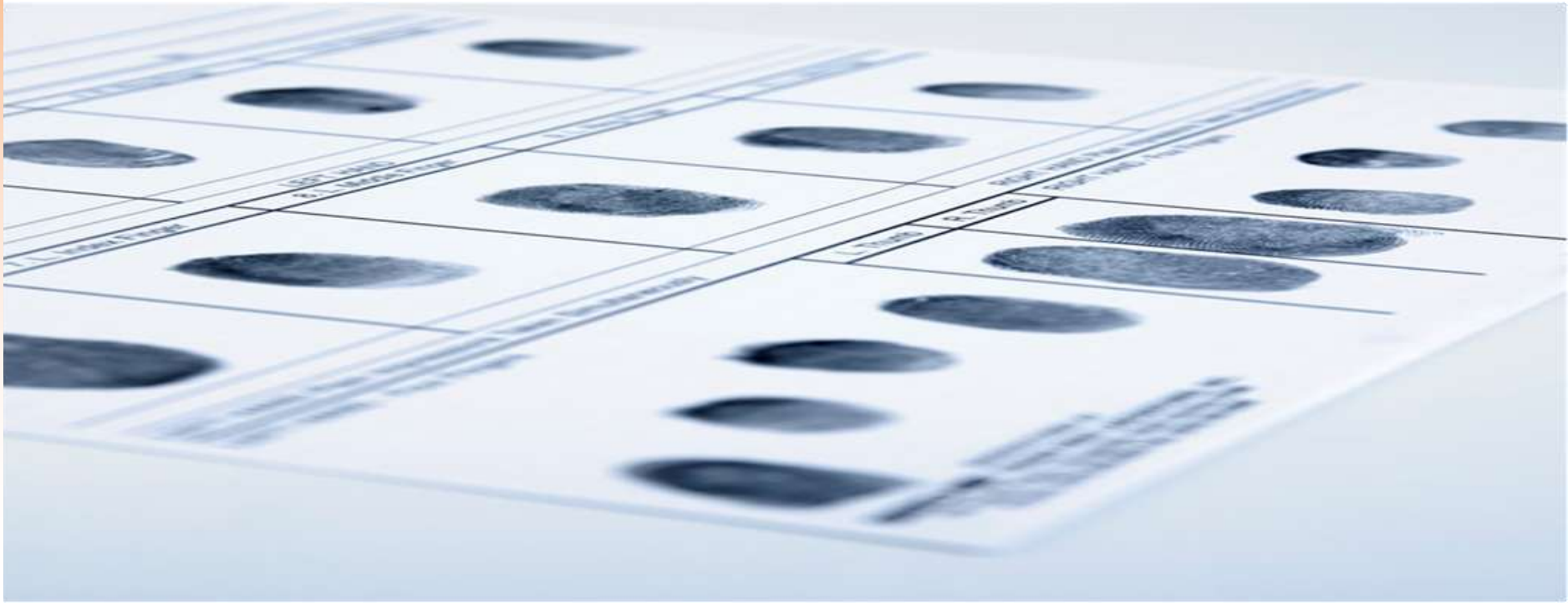
Vulnerabilities and Threats

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
  - Information
  - 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)
  - 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!

Security Awareness Topics

FOR OPERATORS

Individual Accountability

- Every person with access to a CJI system must be “uniquely identified”.
  - Options include (alone or in combination):
    - Full Name
    - Badge Number
    - Serial Number / Personnel Number
    - Other unique alphanumeric identifier
  - Must be unique within the statewide system.

Individual Accountability

- Every person with access to a CJI system must be "uniquely identified" (User ID).
  - The identifier belongs to **YOU**, the individual.
    - **YOU** are responsible for keeping it secure.
    - **YOU** are responsible for every transaction **YOUR** user identifier is used to run.

Password Management

- Passwords serve to authenticate ("prove") your identity to the system.

Password Management

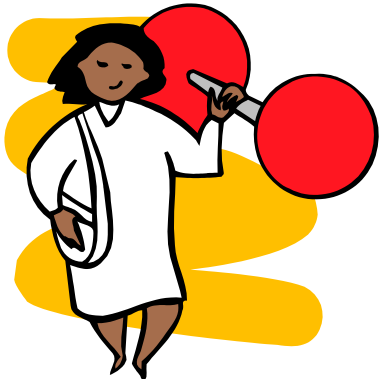
- Your password must be:
  - Minimum of eight (8) characters long;
  - Contain at least one (1) of each of:
    - Upper case character
    - Numeric character
    - Special character
  - Not a dictionary word or proper name;
  - Not the same as your user identifier;
  - Different from your last 10 passwords;
  - Changed every 90 days, or sooner!

Password Management

- What is a strong password?
  - A strong password:
    - Contains digits, symbols, and uppercase and lowercase characters. For example:

      a-z, A-Z, 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./

    - Is at least eight characters long
    - Is not a word in any language, slang, or dialect
    - Is not based on personal information, names of family, etc.



Password Management

Time to crack/hack passwords with respect to password length & complexity (search speed equals 100,000 passwords per second):

Character set / Length	26 (no case, letters only)	36 (no case, letters & digits)	52 (U/L case + letters & digits)	96 (all printable characters)
4 characters	0	0	1 min	13 min
5 characters	0	10 min	1 hr	22 hr
6 characters	50 minutes	6 hrs	2.2 days	3 months
7 characters	22 hrs	9 days	4 months	23 yrs
8 characters	24 days	10.5 months	17 yrs	**2,287 yrs**
9 characters	21 months	32.6 yrs	881 yrs	219,000 yrs
10 characters	45 yrs	1,159 yrs	45,838 yrs	21 million yrs

Password Management

- A secure password is one that is not:
  - Posted
  - Written Down
  - Shared

- Experienced hackers know to look for exposed passwords that are taped to monitors, hidden under keyboards, or even in a desk drawer.

Password Management

- Protect Your Passwords
  - Memorize it
    - Do not put it in writing.
  - Safeguard it
    - Your password is the **key** to one of the most valuable resources.
  - If you forget your password
    - Notify appropriate personnel.
    - Your old password will be deleted from the system and a new one issued.

Password Management

- **DO NOT SHARE YOUR PASSWORD!**
  - Password sharing:
    - Places information that is protected at great risk.
    - Leads to unwanted break-ins by unknown individuals, as well as by known individuals.
  - Your password belongs to **YOU**.
    - **YOU** are responsible for keeping it secure.
    - **YOU** are responsible for every transaction run using **YOUR** password.

Password Management

- When you intend to leave a terminal unattended for any reason, log off or lock your terminal with password protection.

✓ HINT: Press the F12 key in OpenFox Messenger

Password Management

- Immediately following a suspected or known compromise of a system password, a new password must be issued.

`!+S5V-rg`	(Exclamation - Plus - SIERRA - Five - VICTOR - Dash - romeo - golf)
`c8j*z7jM`	(charlie - Eight - juliet - Asterisk - zulu - Seven - juliet - MIKE)
`ZkTS2t%C`	(ZULU - kilo - TANGO - SIERRA - Two - tango - Percentage - CHARLIE)
`dbaUw?3B`	(delta - bravo - alpha - UNIFORM - whiskey - Question - Three - BRAVO)
`%DCFvT23`	(Percentage - DELTA - CHARLIE - FOXTROT - victor - TANGO - Two - Three)
`4gjP#%3&`	(Four - golf - juliet - PAPA - Hash - Percentage - Three - Ampersand)
`=K5A@SAu`	(Equals - KILO - Five - ALPHA - At - SIERRA - ALPHA - uniform)
`BA?B6sNt`	(BRAVO - ALPHA - Question - BRAVO - Six - sierra - NOVEMBER - tango)
`%Cb6qh&w`	(Percentage - CHARLIE - bravo - Six - quebec - hotel - Ampersand - whiskey)
`m6!Rp9QW`	(mike - Six - Exclamation - ROMEO - papa - Nine - QUEBEC - WHISKEY)

Password Management

- When a system user no longer needs access, the password must be removed from the system, and the user identifier must be disabled.

Password Management

When you leave a terminal …

Log off or Lock it.

If you even suspect your password has been compromised …

Change it.

When a user no longer needs access …

Disable the account.

Social Engineering

Every burglar knows that the easiest way to break into a building is to unlock the door with the key.

In the context of computer security, one process of getting the “key” is called social engineering.

Social Engineering

Social engineers don't need to be "technically savvy."

Their "people skills" allow them to gain access to areas they are **NOT** supposed to be through:

- Charm
- Intimidation
- Trickery

Social Engineering

What is Social Engineering?

1. ***Non-technical*** type of intrusion which relies heavily on human interaction and often **involves tricking** other people to break normal security procedures.

What is Social Engineering?

2. *Purposeful manipulation* of an individual or group in an effort **to gain information** or effect certain behavior.

What is Social Engineering?

It may or may not involve technology, but invariably **includes** some form of ***deceit and concealment*** of its actual goal.

What is Social Engineering?

3. Using ***influence*** and ***persuasion*** to deceive people by convincing them that the social engineer is someone he or she is not.

Social Engineering

What is Social Engineering?

As a result, the social engineer is able to ***take advantage*** of people to obtain information with or **without the use of technology**.

Social Engineering

Some Social Engineering tactics:

- "Dumpster Diving"

- Posing as company employees:
  - IT team member
  - Contractor
  - Repairman
  - Janitor

- "Shoulder Surfing"

Psychological Triggers

- Emotional reaction
  - Statement at outset of interaction that triggers strong emotions (fear, excitement, panic, etc.)
  - Disrupts the target individual's normal defenses.
- Overloading
  - Slipping lies in between rapidly delivered truths.

Psychological Triggers

- Deceptive Relationship
  - Establishing an ***apparently*** friendly relationship in order to exploit the target individual.
- Reciprocation
  - Creating a sense of obligation to return a favor.
  - Often used in Reverse Social Engineering.

Psychological Triggers

- Diffusion of Responsibility and Moral Duty
  - Target individual made to feel that he or she will not be held solely responsible for actions.
  - Works well with use of moral duty as motivation.
    - Target individual feels like he or she is doing something to save an employee, to help out the organization, etc.

Psychological Triggers

- Authority
  - People are conditioned to respond to authority.
  - Exploitation by attacker misrepresenting self as an authority figure (director, officer, etc.)

Psychological Triggers

- Integrity and Consistency
  - Exploiting tendency to “do what you say you are going to do”, even if unsure if it is the right thing.
  - Exploiting tendency to believe other’s are telling the truth, unless *strong* evidence to the contrary.

Social Engineering Scenario

Telephoning a user and posing as a member of the IT team, who needs the user's password and other information in order to troubleshoot problems with the network or the user's account.

Social Engineering Scenario

Telephoning the IT department and posing as a high ranking executive in the company, pretending to have forgotten their password and demanding that information immediately because of a pressing business urgency.

"Reverse Social Engineering" Scenario

The social engineer creates a problem on the network or the user's computer.

The social engineer or hacker comes to the rescue, fixes the "problem" thereby gaining the victim's confidence.

Social Engineering

FOREWARNED IS FOREARMED

Don’t be “asleep at the switch.”

Defense Against Social Engineers

Don’t assume personnel know better than to freely give out confidential information.

Defense Against Social Engineers

- Security Awareness Training for all users
  - *Know what has value*
  - *Friends are not always friends*
  - *Know how and when to say "NO"*
  - *Passwords are personal*
  - *Uniforms are cheap*

Defense Against Social Engineers

- Social Engineering Land Mines (SELM)
  - "Please Hold" policy
    - Putting all security requests on hold
    - Gives employee time to consider request validity
  - Call Backs by Policy
    - Should be known telephone number in directory
    - Employee should not give out internal telephone numbers

Defense Against Social Engineers

- Social Engineering Land Mines (SELM)
  - "Key Questions" Strategies
    - "Three Questions" Challenge Rule
      - Users requesting security assistance challenged with any or all of three previously determined questions
      - Questions and answers established at user account creation
      - Answers provided by and known only to actual user
        - "What was the first school you attended?"
        - "What was your father's middle name?"
        - "In what city did you first meet your spouse?"

Defense Against Social Engineers

- Social Engineering Land Mines (SELM)
  - "Key Questions" Strategies
    - "Bogus Question" Gambit
      - Question asked to caller implies false information
        - "I see you work in Legal. How is it to work for Mr. Haney?"
      - Authentic caller likely will set the record straight
        - "Mr. Haney is in Marketing. I work for Mr. Douglas."
      - Hacker builds on the false information and gets "hooked"
        - "Oh, Mr. Haney is a fine boss, and a smart attorney. He is teaching me a lot about integrity."

Defense Against Social Engineers

- Social Engineering Land Mines (SELM)
  - Centralized Security Log
    - Monitored by information security personnel
    - Logging all:
      - Password resets
      - Secure information requests
      - Suspicious calls

Defense Against Social Engineers

- Social Engineering Land Mines (SELM)
  - The Justified Know-it-all
    - A bold social engineer will not hesitate to walk right into an office and start looking around
    - The Justified Know-it-all is a person who:
      - Makes it his or her business to know everyone who is on the floor or walking around in a department
      - Is briefed on security risks of physical intrusion
      - Has power and training to address an unescorted visitor
        - ***Requires support of management to be effective***

Phishing

What is "Phishing"?

- Fraudulent e-mail
  - Masquerading as from a legitimate business:
    - online store or auction site
    - financial institution or online payment provider
    - government agency
    - internet service provider or telephone company
  - Usually claiming to help recipient claim money or prevent problem with account
  - Intention of stealing personal information (**PII**)

Phishing

How does "Phishing" work?

- Fraudulent e-mail
  - Contains legitimate-looking logos and links
    - Address may be altered or misspelled slightly
      - "www.verify-chase.com"
      - "www.mircosoft.com"
      - "www.paypal.mytrick.com"
      - "www.spidersweb.com/bankamerica/login.php?"
    - Address may show only numbers when hovered

Phishing

How does "Phishing" work?

- Fraudulent e-mail
  - Usually claims you need to take urgent action
    - "We need to verify your account to prevent fraud"
    - "Your account is about to be closed"
    - "An order has been placed in your name"
    - "To claim your prize"
    - "The IRS has your refund ready to deposit"
  - Links in e-mail redirect to phony website that looks (nearly) identical to real site

Phishing

How does "Phishing" work?

- Fraudulent e-mail

TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Phishing

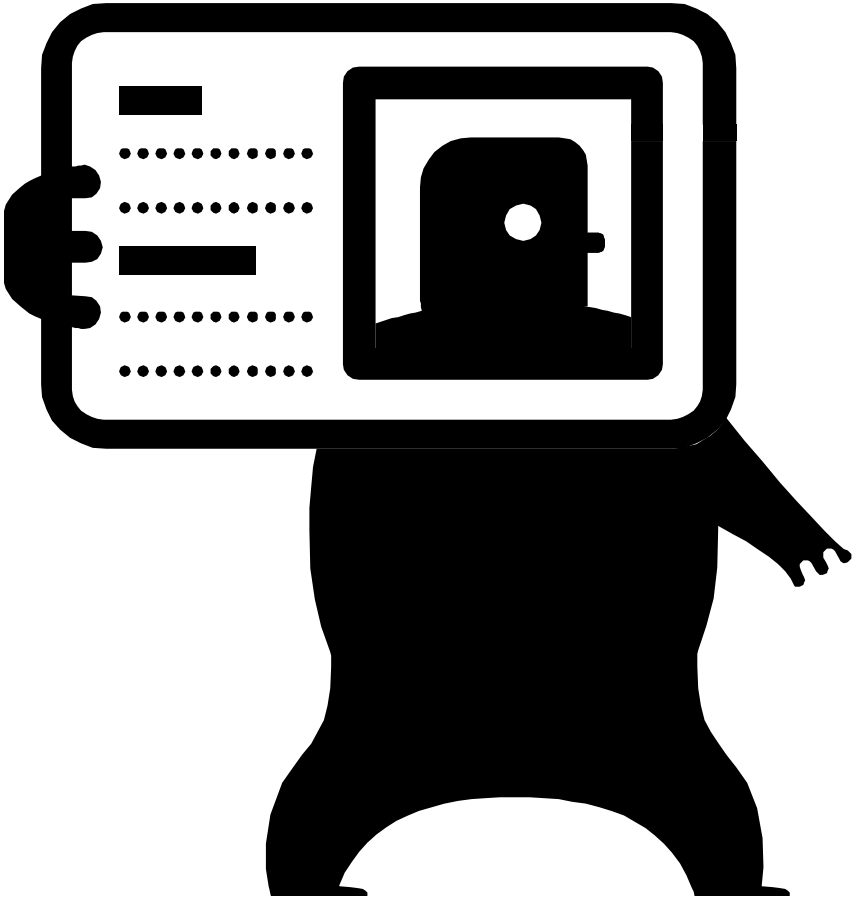
How does "Phishing" work?

- Phony web site
  - Asks for identity information
    - User ID
    - Password
    - Account number
    - Social Security Number
  - May use "pop-up" window in front of legitimate site

Phishing

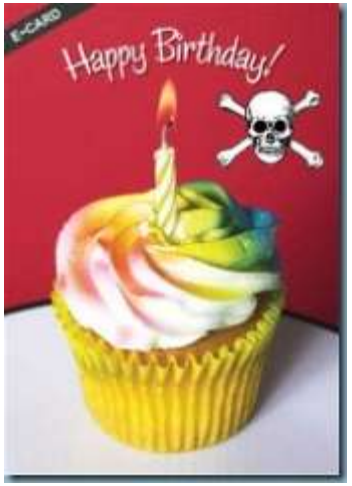
Once a phishing web has your identity …

… <u>you no longer do!</u>



Unknown e-Mail / Attachments

Safe e-Mail Handling



- Suspect any e-mail:
  - From someone you do not know
  - Poorly written or with bad grammar
  - Claiming to be a greeting card, but not telling you who your admirer is
  - With your e-mail address in the “From:” line
  - With random words in the subject line
  - Asking for money or personal information

Unknown e-Mail / Attachments

Safe e-Mail Handling

- Never open attachments that:
  - Are unexpected
  - Have multiple extensions (coolpic.gif.exe)
  - Have dangerous extensions (filename endings)
    - Some common dangerous extensions:

.exe	.pif	.url	.vb	.bas
.bin	.chm	.msi	.vbs	.sct
.com	.scr	.msp	.vbe	.wsc
.cmd	.hta	.inf	.js	.wsf
.bat	.lnk	.reg	.jse	.shs

Unknown e-Mail / Attachments

Safe e-Mail Handling

- Read all e-mail in “plain text” format
  - Does not support imbedded images (tracking)
  - Squashes web-based bugs
  - Prevents attachments automatically opening
- If you know the sender, contact them separately and ask:
  - Did they actually send the e-mail?
  - Was an attachment supposed to be with it?

Spam

What is Spam (other than canned meat)?

- Unsolicited bulk messages
- Various electronic channels
  - e-Mail
  - Instant messaging
  - Mobile phone messaging
- Usually junk commercial advertising
- Often generated by “botnets” – networks of infected computers enslaved to a host

Spam

How to protect against spam

- Guard your e-mail address
  - Do not enter it on an untrusted web site
  - Do not enter it on blogs
  - Use “throw-away” e-mail addresses
- Use junk e-mail filters
- Do not click on “unsubscribe”
  - Often actually confirms your e-mail address

Spam

How to protect against spam

- Never reply to spam
- Delete spam without opening It
- Many e-mail programs delete it or quarantine it for you

Leading Threats to PC Security

Viruses/Worms

Software programs designed to invade your computer, and copy, damage or delete your data

Trojan Horses

Viruses that pretend to be programs that help you while destroying your data and damaging your computer

Spyware

Software that secretly watches and records your online activities or send you endless pop-up ads

Protection from Malware

Types of Malware:

- Infectious
  - Viruses
  - Worms
- Concealment
  - Trojan horses
  - Rootkits
  - Backdoors
- Profit
  - Spyware
  - Botnets
  - Key[stroke] loggers
  - Dialers
  - Malvertising
- Data Stealing

Malware may combine several types

- Botnet replicates via worm through backdoor.

Protection from Malware

- Required for **all** devices on a CJI network.
- Several **FREE** options available:
  - Avast! Free Antivirus
  - AVG Anti-Virus Free Edition
  - Avira AntiVir Personal
  - Malwarebytes Anti-Malware
  - Microsoft Security Essentials
  - PC Tools Antivirus Free
  - ZenOK

Protection from Malware

Use an Internet Firewall

An Internet firewall is like a moat around a castle, creating a barrier between your computer and the Internet.

(Ask your IT department if you need help setting up your PC's firewall.)

Access Control

- Access Control comprises:
  - Account Management
  - Access Enforcement
    - Least Privilege
    - System Access Control
    - Access Control Criteria
    - Access Control Mechanisms
  - Unsuccessful Login Attempts
  - System Use Notification
  - Session Lock

Access Control

- Account Management requires
  - **Agencies must have** policies established and followed for:
    - Creating/activating/modifying accounts
    - Reviewing/validating accounts
    - Disabling/removing accounts

Access Control

- Account Management requires
  - Accounts/access granted based on:
    - Valid need-to-know/need-to-share determined by assigned official duties
    - Meeting all relevant personnel security criteria
      - Fingerprint-based background check
      - No felony convictions
      - Reviewed by CSO if any other record exists

Access Control

- Account Management requires
  - Local agency must notify CSA when:
    - User's need-to-know/need-to-share CJI changes
    - User is terminated or transferred
    - User accounts are removed, disabled, or otherwise secured against use

Access Control

- Access Enforcement involves:
  - Least Privilege
    - Granting users only the level of access they need to do their job, and nothing more.
    - CJI access limited to personnel with the right and need to know.

Access Control

- Access Enforcement involves:
  - System Access Control
    - Preventing users from logging on to multiple concurrent sessions.
    - Ensuring only authorized personnel can add, change, or remove component devices, dial-up connections, and remove or alter programs.

Access Control

- Access Enforcement involves:
  - Access Control Criteria
    - Job assignment or function (i.e., role-based.)
    - Network addresses or Physical/Logical location (users from sites within an agency may be permitted greater access than those from outside.)
    - Time-of-day and day-of-week/month restrictions.

Access Control

- Access Control comprises:
  - Unsuccessful Login Attempts
    - No more than five consecutive attempts to logon
    - Accounts must be locked for 10 minutes after five unsuccessful attempts
    - All unsuccessful attempts logged

Access Control

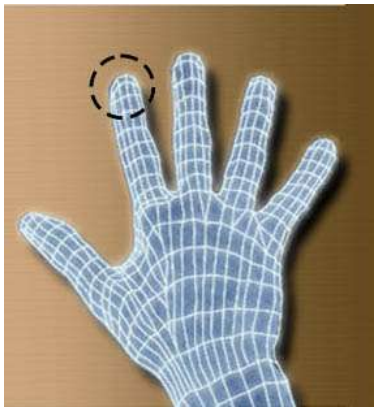
- Access Control comprises:
  - System Use Notification – message at logon that states
    - User is accessing a restricted information system
    - Usage may be monitored, recorded, and audited
    - Unauthorized use of the system is prohibited and may be subject to criminal and/or civil penalties
    - Using the system consents user to monitoring

Access Control

- Access Control comprises:
  - Session Lock
    - Automatically lock after 30 minutes of inactivity
    - User must use lock whenever station unattended
    - Not required for
      - Dispatch stations
      - Devices that are ***part of*** a police vehicle
        - When device is removed from a police vehicle, lock must be used and automatic.

Advanced Authentication

- Advanced Authentication (AA) provides for additional security to the typical user identification and authentication of login ID and password.



Advanced Authentication

- Advanced Authentication (AA) is always in addition to a user ID and password; it does not replace them.

Advanced Authentication

- Advanced Authentication (AA) includes:
  - Biometric systems (fingerprint/retina readers)
  - User-based public key infrastructure (PKI)
  - Smart cards
  - Software tokens
  - Hardware tokens
  - Paper (inert) tokens (i.e. “bingo cards”), and

Advanced Authentication

- Advanced Authentication (AA) includes:
  - "Risk-based Authentication", which uses:
    - A software token element comprised of:
      - Network information
      - User information
      - Positive device identification
        - device forensics
        - user pattern analysis
        - user binding
    - User profiling, and
    - High-risk challenge/response questions

Advanced Authentication

- Advanced Authentication (AA) IS required:
  - When accessing criminal justice information (CJI) from a location that is NOT physically secure.
    - For instance,
      - A motorcycle police officer using a handheld device to run Driver and Registration checks is *required* to authenticate using AA.
      - A detective using a notebook computer from a hotel room is *required* to authenticate using AA.

Advanced Authentication

- Advanced Authentication (AA) is NOT required:
  - When accessing criminal justice information (CJI) from a physically secure location.
    - For instance,
      - AA is NOT required when a detective accesses the system from within a police station.
    - NOTE: For the sole purpose of meeting the advanced authentication policy, a police vehicle shall be considered a physically secure location until September 30, 2013.

Advanced Authentication

- Advanced Authentication (AA) waived until September 30th 2013, **IF**:
  - Device associated with and located in a police vehicle, **AND**
  - The information system used has not been procured or upgraded significantly anytime after September 30th, 2005;

OR

Advanced Authentication

- Advanced Authentication (AA) waived until September 30th 2013, **IF**:
  - Agency has funded or implemented Internet Protocol Security (IPSec; aka Secure VPN) in order to meet the AA requirements of CJIS Security Policy v.4.5.
- EXCEPTION:
  - AA shall be required when the system has built AA into its processes and requires a user to provide AA before granting access.

Encryption

- Encryption is required when …
  - CJI is transmitted outside of a "physically secure location", for example –
    - Shared county government network
    - Networks not owned and managed by a CJA
    - Any wireless networks
  - CJI is "at rest" (i.e. stored electronically) outside of a "physically secure location" –
    - USB drives or portable hard drives
    - Laptop computers

Encryption

- Encryption must be …
  - ***Minimum*** of 128-bit strength
  - DES-3 or AES (*preferred*)
  - Federal Information Processing Standard (FIPS) 140-2 ***Validated***

    (*see* http://csrc.nist.gov/groups/STM/cmvp/validation.html, *and* http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm)

Web Usage

CJI systems, including workstations, are the property of your agency or employer.

- CJIS systems are **F**or **O**fficial **U**se **O**nly.
- Agencies may restrict access to the web.
- Agencies may restrict certain web sites.
- Agencies may monitor web and e-mail.
- **Do not expect privacy in your usage.**

Stay safe … surf the Web at home!

Publicly Accessible Computers

- Publicly accessible computers
  - Such as:
    - hotel business center computers
    - convention center computers
    - public library computers
    - public kiosk computers
  - shall not
    - access
    - process
    - store, or
    - transmit

Criminal Justice Information

Personally-Owned Equipment

- Personally-owned equipment
  - Such as:
    - your laptop computer
    - your home workstation
    - your smart phone
    - your handheld computer (PDA)
    - your USB drive
    - your rewritable CD
  - shall not
    - access
    - process
    - store, or
    - transmit

Criminal Justice Information

Desktop Computer Security

- NCIC terminals are **FOUO** – "**F**or **O**fficial **U**se **O**nly."

- NCIC terminals must be operated only within controlled spaces and under the direct supervision of authorized personnel.

Desktop Computer Security

- Physically position your computer away from public or unauthorized viewing.
- When not under the direct supervision of an authorized person either during or outside regular working hours, NCIC terminals must be:
  - Turned off; and
  - All diskettes, tapes, removable hard-disks and USB drives, and printer ribbons must be removed and secured.

Notebook Computer Security

- Personal firewall required
- Maintain physical security
- Secure wireless communications
  - WPA2 – Wi-Fi Protected Access v.2
  - FIPS 140-2 ***Validated***
- Encrypt hard drive/storage devices
- Use advanced/two-factor authentication
  - "Something you have + something you know"
  - User ID + password ***is not enough***

Handheld Device Security

- Same as notebook computers
- Encrypt **all CJI** on the device
- Erase cached information
- Use local device authentication

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 System Operators

- 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 operating directly, or otherwise am handling, exposed to, or have access to information 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