CJIS
Information Security Awareness Training for Texas

Objectives

- This Information Security Awareness Training is designed to equip those who access the data that moves through TLETS with basic tools needed to protect computers and networks interconnecting with Criminal Justice Information Services (CJIS).
- To ensure compliancy for each agency, security awareness training is required within six months of employment and every two years thereafter for all employees who access CJIS data. This requirement applies to IT personnel as well as vendors who work with networking equipment and/or software which stores and/or transmits CJIS data.
- **The first step to achieving security is awareness.**

Overview

In the following Security Awareness Training Document, the following ideas will be discussed.

Terms and Definitions
Information Systems
Information Technology Security
- *Goals*
- *Viruses and Reports, Spam*
- *Robust Passwords*
- *Password Security*

Physical Security
Personnel Security
Sensitive Data
- *Storing*
- *Securing*
- *Vulnerabilities and Threats*
- *Social Engineering*
- *Reporting Security Violations*
- *Dissemination*
- *Standards of Discipline*
- *Disposal*

Summary
CJIS Security Office Contacts

List of terms

- Access
- Authorized Personnel
- CCH
- CJI
- CJIS
- CHRI
- III
- LASO
- NCIC
- NLETS
- Phishing
- PII
- TCIC
- TLETS

Terms and Definitions

Access – defined as “the opportunity to make use of an automated information system resource. Includes the ability to have contact with a computer from which a transaction may be initiated.”

Authorized Personnel – defined as “those persons who have passed a state and national finger print based background record check and have been granted access.” These individuals take security awareness training upon hire and every two years thereafter to keep current.

Terms and Definitions

CCH - The **C**omputerized **C**riminal **H**istory System is Texas' central repository for arrest, conviction, and disposition data on individuals arrested for felony and gross misdemeanor offenses. It is used by criminal justice agencies for a variety of reasons, including decisions regarding investigations, arrests, criminal charges, plea bargains, convictions, probation, and placement in correctional facilities. It is frequently used during mandated background checks on individuals seeking employment or licensing for various employed and volunteer positions.

Terms and Definitions

CJI – Criminal Justice Information refers to data provided by FBI CJIS necessary for law enforcement and civil agencies to perform their mission. Examples of CJI data sets housed by the FBI include:

1. Biometric Data – used to identify individuals; may include: palm prints, DNA, iris, facial recognition data as well as fingerprints.
2. Identity History Data – text data that corresponds with an individual's biometric data, providing a history of criminal and/or civil events for the identified individual.

Terms and Definitions – CJI (continued)

3. Person Data – information about individuals associated with a unique case, and not necessarily connected to Identity History Data. Person Data does not provide a history of an individual, only information related to a unique case.
4. Property Data – information about vehicles and property associated with crime.
5. Case/Incident History – information about the history of criminal incidents.

Terms and Definitions

- **CJIS - Criminal Justice Information Services** is home to a range of state-of-the-art technologies and statistical services that serve the FBI and the entire criminal justice community. CJIS systems include, but are not limited to:
- National Crime Information Center (NCIC)
- Uniform Crime Reporting (UCR)
- Automated Fingerprint Systems (AFIS)
- National Instant Criminal Background Check System (NICS)
- Interstate Identification Index (III)
- Law Enforcement Online (LEO)
- National Data Exchange (NDEx)
- National Incident-Based Reporting System (NIBRS)

Terms and Definitions

CHRI - Criminal History Record Information is a subset of CJI that consists of notations and/or written and/or electronic evidence of an arrest, detention, complaint, indictment, information or other formal criminal charge relating to an identifiable person. CHRI includes identifying information pertaining to the individual as well as the disposition arising from sentencing, correctional supervision, and release of any charges. CHRI is collected by criminal justice agencies and provided to the Texas Department of Public Safety, Crime Records Service (DPS CRS). DPS CRS is responsible for compiling, maintaining and disseminating complete and accurate criminal history records, criminal incident reports, arrest reports and statistics. CHRI is not only accessed by criminal justice agencies, but is also available to non-criminal justice entities. Background check requests are obtainable in two forms: 1) A personal identifier or name-based search which obtains information based on name and a numeric identifier and 2) Fingerprints.

Terms and Definitions

III ("Triple-I" for short) - is the **Interstate Identification Index**. The CJIS service that manages automated submission and requests for CHRI that is warehoused subsequent to the submission of fingerprint information. III holds the FBI's compilation of an individual's criminal identification, arrest, conviction, and incarceration information. III provides the FBI's RAP sheet (Record of Arrest and Prosecution) and contains information reported by local, state and federal law enforcement agencies across the country. Requests associated to a record housed in a particular state are directed to the originating State as needed.

Terms and Definitions

LASO – **The Local Agency Security Officer** is required to be appointed to guarantee five areas of information for audit purposes:

1. Identify who is using the approved hardware, software and firmware and ensure no unauthorized individuals or processes have access to the same
2. Identify and document how the equipment is connected to the state system
3. Ensure personnel security screening procedures are being followed
4. Ensure the approved and appropriate security measures are in place and working
5. Support Policy compliance and keep state and federal ISO informed of security incidents

Terms and Definitions

- The LASO is appointed by the local agency. For audit purposes, DPS requires the LASO to be able to:
- Identify who is using the approved hardware, software and firmware and ensure no unauthorized individuals or processes have access to the same
- Identify and document how the equipment is connected to the DPS
- Ensure personnel security screening procedures are being followed
- Ensure the approved and appropriate security measures are in place and working
- Support policy compliance

Terms and Definitions

NCIC - The **National Crime Information Center** is "a computerized index of documented criminal justice information concerning crimes and criminals of nationwide interest" which includes "a locator file for missing and unidentified persons." NCIC stores information regarding open arrest warrants, stolen property, missing persons, etc. and is available to federal, state, and local criminal justice agencies 24 hours a day, 365 days a year.

Terms and Definitions

Nlets - the **International Justice and Public Safety Network** (formerly known as the National Law Enforcement Telecommunications System) links together state, local, and federal law enforcement, criminal justice and public safety agencies for the purpose of exchanging critical information necessary to support the men and women of law enforcement. This interface can provide information from each state's criminal records, driver records, vehicle registration records, INTERPOL, Immigrations and Customs Enforcement (ICE), License Plate Reader (LPR) records, national Amber Alerts, Hazardous Waste mobile tracking, National Weather Service, and much more. Nlets is available 24 hours a day, 7 days a week, 365 days a year.

Terms and Definitions

Phishing – In the field of computer security, is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. Phishing is typically carried out by e-mail or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Even when using server authentication it requires skill to detect that the website is fake. Phishing is an example of social engineering techniques used to fool users, and exploits the poor usability of current web security technologies.

Terms and Definitions

PII – Personally Identifiable Information is information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. PII includes, but is not limited to: education; financial transactions; medical, criminal or employment history. Information derived from CHRI is usually PII.

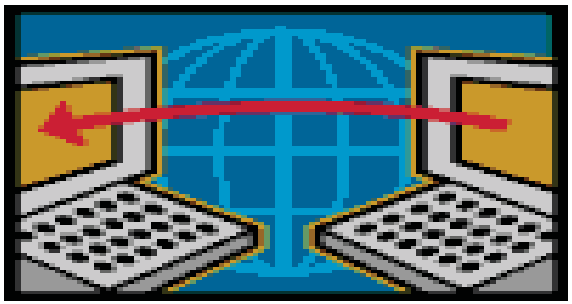
Terms and Definitions

TCIC - the **Texas Crime Information Center** contains criminal justice information regarding wanted persons, missing persons, unidentified persons, sex offenders, persons subject to protective orders, stolen vehicles and boats, handgun licenses, abandoned/recovered vehicles and boats, H.E.A.T. vehicles, identity theft, child safety checklist, threat against peace and detention officers, etc. Law enforcement and criminal justice agencies may access TCIC 24 hours a day, 7 days per week to maintain or obtain status concerning property and person records stored in the repository.

Terms and Definitions

TLETS – the **Texas Law Enforcement Telecommunications System** is a critical statewide network combined with multiple distributed applications that provides message brokering services, a client application, and operational software. TLETS is the primary access for local criminal justice agencies in Texas to criminal justice information provided by TCIC, NCIC, DMV, Driver License, other states via Nlets, CCH, III, etc. TLETS also acts as a secure information exchange system between law enforcement and criminal justice agencies within Texas and between agencies nationwide. DPS strives to provide TLETS services 24 hours a day, 7 days a week.

Information System



To understand the importance of information system security or information technology security, an information system needs to be defined.

The term “information system” means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of CJI or PII information.

Since individuals, businesses, and government organizations have become increasingly reliant on information technology systems, everyone is affected which makes protecting these assets more important than ever.

Information Technology Security The Goal !

Computer systems have become more complex and interconnected, increasing the potential risk with their operations. Because of this complexity, protecting Information Technology Security systems from unauthorized access, use, disclosure, disruption, modification, or destruction must have three criteria:

Confidentiality: to ensure that information is not disclosed to unauthorized individuals.

Integrity: to make sure that information and systems are not modified maliciously or accidentally.

Availability: the reliability and timely access to data and resources by authorized individuals

Information Technology Security

Risks and Actions

Computer systems have become more complex and interconnected, increasing potential risk for security breaches. Protecting information systems from unauthorized access, use, disclosure, disruption, modification, or destruction is important. Three topics being addressed here are:

- Viruses
- Spam
- Password Security

Viruses

What is a virus?

- A virus is software that is used to infect a computer. A destructive virus may destroy programs or data immediately or lie dormant and be scheduled to be triggered based on an event such as a particular date and time. Viruses are often used to infect systems in order to compromise the computer or the data residing on the computer.

Where do viruses come from?

- Malicious websites, email and portable drives are a common source of computer virus infections.

Viruses

Virus Security

- Though not 100% effective, using the most recent antivirus software with updated signature files is required by the CJIS Security Policy. Use automatic updates for Operating System Patches, Antivirus Software, and Antivirus signature files to be most effective. Ensure that workstations, network equipment and servers are protected from virus threats and scanned regularly.

What could happen if a virus is acquired?

- Some viruses can be broadcast throughout a network to infect other computers. This could put all computers interconnecting through TLETS and Nlets at risk and could compromise nationwide law enforcement communications.

Your Virus Response

What must occur when a virus is detected?

- When a virus incident occurs, the following process must be followed:
- Determine which agency will handle TLETS traffic while the problem is being attended to.
- **Immediately** call DPS at 1-800-63-TLETS and select option 2. Upon reaching a technician, a report will be generated.
- Disconnect the Ethernet cable from the computer or router
- As a precautionary measure, DPS will disable the local agency from access to the TLETS network until IT personnel can guarantee systems are free from infection. Once free from infection, the agency will be reconnected to TLETS.
- **DPS is eager to assist in securing a timely solution to all virus incidents.**

Reporting what happens

Reporting What Happens

- While on the phone with TLETS personnel, it will be necessary to provide information necessary to prepare a report on the issue. This is necessary for the following reasons:
- To document the incident at DPS.
- To provide the local agency chain of command and IT staff with information related to the incident.
- To comply with the requirement to communicate all security incidents to FBI CJIS.
- **So what is on the report?**

Report: 12 Questions

- Name (if known) of virus.
- Was Antivirus software running at the time of infection?
- How and when was it first identified?
- Has Local IT staff been notified/are they involved?
- Number of workstations infected?
- Any other equipment infected?

Report: 12 Questions continued

- Action plan for removal.
- Will infected workstations be re-imaged before reconnection?
- When was the last update of signature files?
- When was the last operating system update?
- Was any CJIS data or personnel identification information compromised?
- Is there anything the agency needs the Security Office to do to help?

Spam

Spam is the name given to unsolicited bulk email that appears in your inbox. Most Spam is advertising from dubious products, get-rich-quick schemes, or other attempts to get money from you and /or infect your computer.

NEVER open unsolicited email, click on any emails or attachments, nor reply to emails from an unknown source.

Passwords

- The TLETS Omnixx end user is required to provide his or her user ID and password to authenticate into the TLETS system. Interface systems are required to authenticate TLETS end users within their application.
- In either case, the CJIS Security Policy requires robust passwords to be used for all persons with CJI data access.
- Each transaction submitted through TLETS must be uniquely identified by the requestor’s user ID as assigned by Texas DPS.

Robust Password Construction Assistance

Following is a recommendation for the development of robust passwords. The recommendation is divided into three sections.

1. Do’s
2. Don’ts
3. Base Password Construction

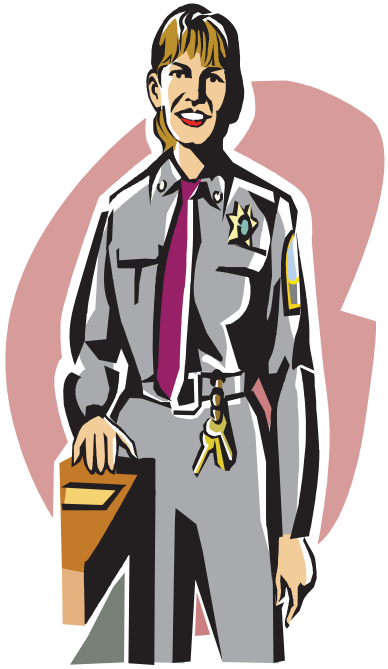
DO!

Robust password components:

Use a minimum of 8 characters

Include characters from the following classes:

- Letters (upper and lower case)
- Numbers
- Special Characters



Make it appear to be a random sequence of letters and numbers

DON’T !

Don't use:

x - any part of your logon name.
x - any word in the dictionary
x - any portion of your previous password
x - repeating sequence of letters or numbers
x - adjacent keys on the keyboard like "qwerty“
x - numbers in place of similar letters "0 for o, 1 for l“
x - all numbers
x - all letters
x - proper nouns (including names)
x - other information about you like license plate, telephone number, street address, etc.

Create Base Password

Following is a recommendation that can be used to create a base password. Create a base password from a phrase describing your likes or preferences; a memorable event in your life; or a line from a favorite song, poem, or book. Take the first letter (or one or two letters) from each (or some) of the words to create the basis for your password.

For example if the phrase is "I **l**ove to **w**alk in the **p**ark on a **s**unny **d**ay", you might select "**lwpsd**" as the base word. Create a base password by alternating between one consonant and one or two vowels, up to six characters. This provides nonsense words that are usually pronounceable, and thus most easily remembered.

With the created base password of "**lwpsd**“, apply capitalization, add numbers and special characters which could yield, for example, "**L2W#p+sd**“

Password Security

Sharing passwords compromises protected information and increases the possibility of unwanted break-ins from known and unknown sources.

A secure password is never:

Posted
Written Down
Shared

Password Security

Experienced hackers and auditors know some individuals keep passwords taped to monitors, hidden under keyboards, placed in a desk drawer, etc.

Memorize your password - do not put it in writing

Safeguard your password - you are responsible for its usage

If you forget your password, notify appropriate personnel; your old password will be deleted from the system and a new one issued

Physical Security

The CJIS Security Policy requires that all computers with TLETS access be protected from any unauthorized access or routine viewing.

This includes network devices, access devices, handheld devices, laptops in vehicles or other outside locations, printed data or stored data.

Equipment must be kept in a secured location accessed and viewed only by authorized personnel.

How to Achieve Physical Security

- TLETS computers must be physically positioned so all unauthorized persons are not able to observe the keystrokes or view the screen.
- Personnel who are going to be away from their desk or police vehicle must render their computer inaccessible.
- Some applications have a “quick lock” key; barring that, systems should be shut down or locked. For Windows-based workstations, lock the system by pressing the Ctrl-Alt-Delete keys simultaneously, then click on “Lock Computer”.

Additional Roles for select IT folks

In addition to all of the physical and technical security – network, security and system administrators must address the following:

- Antivirus updates and definitions
- Data Backup and storage – centralized or decentralized
- Timely application of system patches – part of configuration management
- Access control measures
- Network infrastructure protection measures

For more information on this read 5.2. of the Policy and Annex I

Lost or Stolen Computers

If your TLETS computer or your vehicle with an MDT/MDC is lost or stolen, it is imperative to notify your Local Agency Security Officer or your Terminal Agency Coordinator (TAC) immediately.

Your local procedures may call for other people in your agency to be notified as well.

Personnel Security

State of residency and a national finger print-based background check shall be conducted within 30 days of employment or assignment

Personnel who are not fingerprint-based background checked are considered to be unauthorized and must be escorted by authorized personnel at all times while visiting any area that has computers or network equipment which run Criminal Justice Information.

Sensitive Data

Crime scenes are no longer only at muggings or robberies

Today's crime scene may be in your:

- Living room
- Home office
- Workplace

Storing Sensitive Data

Criminals no longer have to break through a window or pick a lock to invade your privacy. They can enter via the internet and remove the personal information that you have stored for private use, believing it to be safe.

The objective of the hacker is to break into the computer and steal your information; so it is very important that intrusion is made to be as difficult as possible.

Securing Sensitive Data

Ways to protect your vital information

- Make sure the computer system is protected with a robust password
- Make sure the computer is up to date with patches (operating system and applications)
- Practice smart internet habits when performing financial transactions on line. Be selective of the sites you visit and check for the security level of web pages that require you to enter personal information
- When entering personal information on a website verify the website is encrypted. On a web browser window the lock should appear. This lock signifies that the website is encrypted
- Another indication that the site is secured is located in the address line in the browser window. Look for an address that starts with https://

Security Vulnerabilities

A vulnerability is a point where a system is susceptible to attack. Vulnerabilities may include:

Physical Attacks

Natural Disasters

Media Compromises

Human Error

Miscommunications

Hardware and Software Issues

Natural and Unintentional Threats

Natural: Fire, Flood, Lightning, Power Failures

Unintentional: Physical damage to equipment, inadvertently deleting information, permitting unauthorized users access

Intentional Threats

<u>Intentional</u> threats include:

Social Engineering

Phishing

Sabotage

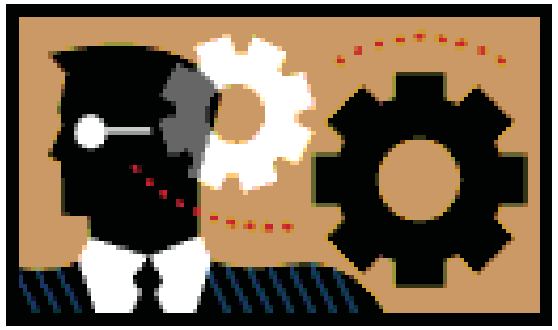
Eavesdropping

Unauthorized Data Access

Intrusions

Denial of Service

Theft



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 do not need to be “technically” savvy.

Their “people skills” get them in where they are **NOT** supposed to be by using:

Charm
Intimidation
Trickery

Social Engineering

- How does Social Engineering work?

Definition:

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

Social Engineering

Social Engineering Scenarios:

#1

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

Social Engineering Scenarios:

#2

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

Social Engineering

Social Engineering Scenarios:

#3

Developing a personal relationship with a user or IT team member with the intent of “sweet talking” the person out of confidential information that can be used to break into the network

Social Engineering

Some Social Engineering tactics:

“Dumpster Diving”

Posing as company employees:

- IT team member
- Building repair personnel
- Janitors

“Shoulder Surfing”

Social Engineering

"Reverse Social Engineering"

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

Then, the social engineer or hacker comes to the rescue, fixes the "problem" and, thereby, gains the victim's confidence.

Social Engineering

Defense Against Social Engineers

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

Some personnel have no reason to question another employee who seem to have a legitimate need.

Even IT team members (who are security-conscious) may trust an irate person claiming

to be upper management.

Social Engineering

- Social engineering could be considered the easiest way for a hacker to access any network and one of the most common hacking tools.
- As a rule, most companies do nothing to prevent exploitation of the human factor.
- Establishing policies is the first step in preventing socially engineered attacks.
- The most important step is to educate personnel to make them aware of the danger of social engineering.
- People who fall prey to social engineering scams are those who haven’t heard about them.

Social Engineering

FOREWARNED IS FOREARMED

Don’t be “asleep at the switch”. Visitor control, challenging strangers, and reporting unusual activities are critical to the safety of CJIS data.

REPORT SECURITY VIOLATIONS

If you become aware of any policy violation or suspect that your password may have been used by someone else, first, change your password and, then, report the violation immediately to your Local Agency Security Officer (LASO) or Terminal Agency Coordinator (TAC).

Sensitive Data Dissemination

CHRI from either the state or federal repositories may only be used for an authorized purpose, consistent with the purpose for which the system was accessed. Dissemination to another agency is authorized if the other agency is an authorized recipient (i.e. has an Originating Identifying Number (ORI)) of such information and is being serviced by the accessing agency.

Security Policy for each Agency

- Each law enforcement agency decides whether personally owned equipment or software may be connected to CJIS systems
- Depending upon how advanced authentication is employed, whether mobile systems will be used in secured or non-secured locations
- Depending upon what Inter-agency agreements and Management Control Agreements are signed and put in place, emergency management functions may vary.

Standards of Discipline

Information contained within the FBI CJIS Information System is sensitive information. Improper access, use and dissemination are serious and may result in the termination of system access, imposition of administrative sanctions, and possibly state/federal criminal penalties.

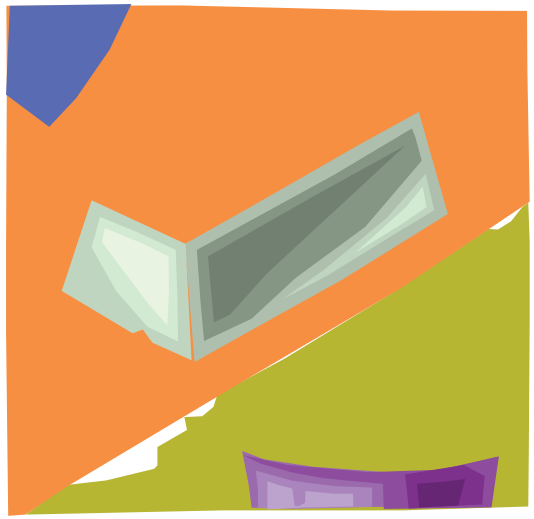
Disposal of Sensitive Data

When no longer using diskettes, tape cartridges, ribbons, hard copies, print-outs, and other similar items, simply destroy them by shredding, destroying, or burning.

DO NOT PLACE SENSITIVE DATA IN TRASH CANS

Disposal of Media

- Shred



- Destroy

- Burn

Summary

“You are the key to security, it begins with you”

It is everyone’s responsibility to ensure they are aware of and adhere to all policies and procedures regarding IT Security

If there are any questions about the proper operation or security of computer systems, contact your LASO or TAC

To report any issues please contact the Travis County Sheriff's Office LASO directly:

LT. ROBIN OSBORN
512.854.4809 (office)
512.854.9189 (fax)