CJIS
Information Security Awareness Training for Texas

Objectives

- This Information Security Awareness Training is designed to equip those accessing the agency's data with basic tools to protect computers and networks interconnecting with Criminal Justice Information Services (CJIS).

- To ensure compliance with federal and state policies, security awareness training is required within six months of employment and every two years thereafter for all employees who may access CJIS data. This requirement applies to vendors also who work with networking equipment and/or software which stores, processes, or transmits CJIS data.

Special note for CJIS Security Policy section 5.2 requirements -

- Level I, II, III training objectives will be presented here only.
- Level IV IT training objectives are available through the CJISonline training module. https://www.cjisonline.com

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
Contacts

List of Terms

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

Terms and Definitions

Access – 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. Access includes physical and logical access to data, and the systems that process, store and transmit data.

Authorized Personnel – Personnel who have passed a state and national finger print based background record check and have been granted access.

Terms and Definitions

CCH - The **C**omputerized **C**riminal **H**istory System is the Texas central repository for arrest, conviction, and disposition data on individuals arrested for felony and gross misdemeanor offenses. Criminal justice agencies access this data for a variety of reasons, regarding decisions on investigations, arrests, criminal charges, plea bargains, convictions, probation, and placement in correctional facilities.

This data is frequently used during mandated background checks on individuals seeking employment or licensing for various employed and volunteer positions.

Terms and Definitions

CJI – Criminal **J**ustice **I**nformation 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.

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 **J**ustice **I**nformation **S**ervices 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)
- Multimodal Biometric Identification System (MBIS)
- National Instant Criminal Background Check System (NICS)
- Interstate Identification Index (III)
- Law Enforcement Enterprise Portal (LEEP)
- National Data Exchange (N-DEx)
- National Incident-Based Reporting System (NIBRS)

Terms and Definitions

CHRI - Criminal **H**istory **R**ecord **I**nformation is a subset of CJI consisting of notations written and 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.

DPS Crime Records Service (CRS) is responsible for compiling, maintaining and disseminating complete and accurate criminal history records, criminal incident reports, arrest reports and statistics.

Terms and Definitions

III ("Triple-I") - **I**nterstate **I**dentification **I**ndex. 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.

Terms and Definitions

LASO – **L**ocal **A**gency **S**ecurity **O**fficer is 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

NCIC - National **C**rime **I**nformation **C**enter 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- International Justice and Public Safety Network

(aka National Law Enforcement Telecommunications System) is a computer-based message switching system that links together and supports every state, local, and federal law enforcement, justice, and public safety agency for the purposes of sharing and exchanging critical information.

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 more. NLETS is available 24 hours a day, 7 days a week, 365 days a year.

Terms and Definitions

Phishing – 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 often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate website. Phishing is an example of social engineering techniques used to fool users, and exploits poor web security technologies.

Terms and Definitions

PII – Personally **I**dentifiable **I**nformation 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 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 usually contains PII.

Terms and Definitions

TAC - **T**erminal **A**gency **C**oordinator is the individual serving as the point-of-contact at the local agency with DPS for matters relating to CJIS information access. The TAC administers CJIS systems programs within the local agency and oversees the agency's compliance with CJIS system policies.

Terms and Definitions

TCIC - Texas **C**rime **I**nformation **C**enter 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 – Texas **L**aw **E**nforcement **T**elecommunications **S**ystem 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 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

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 Goals

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 information is not disclosed to unauthorized individuals.

Integrity: to ensure 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.

The next three topics are:

- Viruses
- Spam
- Password Security

Computer Viruses

What is a computer virus?

- A virus is software 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 computer viruses come from?

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

Computer Viruses

Computer Virus Security

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

What could happen if a computer 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.

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 email attachments from unknown sources, nor reply to emails from an unknown suspicious source.

Your Virus Response

What must occur when a virus is detected?

- When a virus incident occurs, the following process shall be followed:
- Determine which agency will handle TLETS traffic while the problem is being attended to.
- **Immediately** call 1-800-63-TLETS and select option 2. Upon reaching a technician, a report will be generated.
- Disconnect the Ethernet cable from the computer, if possible.
- **Do not unplug the power cord, the system may not restart.**
- Follow your agency's Incident Response Plan
- As a precautionary measure, DPS will disable the system from access to the TLETS network until IT personnel can guarantee systems are free from infection. Once free from infection, the system will be reconnected to TLETS.

Report What Happens

Reporting What Happens to DPS

- 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 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: Questions

- What is virus name, if known?
- Was anti-virus software running at the time of infection?
- How and when was virus first identified?
- Has Local IT staff been notified/are they involved?
- Number of workstations infected?
- Any other equipment infected?
- What action plan for removal is in place?

Report: Questions

continued

- Will infected workstations be re-imaged before reconnection?
- When was the last anti-virus signature update?
- When was the last operating system update?
- Was any CJIS data or personal identification information compromised?
- Is there anything the agency needs the CJIS Security Office to know to help?

Passwords

- A TLETS user account and password is required to authenticate into the TLETS system.
- The CJIS Security Policy requires robust, complex passwords of eight characters or more to be used for all persons with network access.
- Do not transmit passwords in clear text outside the secure location.
- Each transaction submitted through TLETS must be uniquely identified by the requestor's Login ID. Login IDs are *not* shared by personnel.

Robust Password Construction Assistance

Following is a recommendation for developing a robust password. The recommendation is divided into three sections.

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

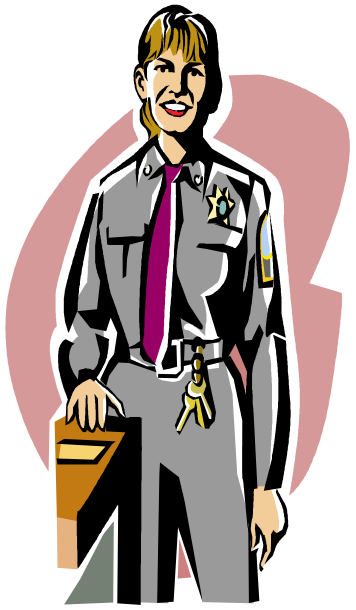
DO!

Robust password components:

Use 8 characters or more

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 or 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 **like** to **ride** my **bicycle** on a **s**unny **d**ay", you might select “**lrbsd**” 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 “**lrbsd**”, apply capitalization, add numbers and special characters which could yield, for example, “**L2R!b+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
- Displayed on screen when entered

Password Security

- Experienced hackers and auditors know passwords are 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
- Change your password every 90 days or less
- Passwords must be unique for 10 iterations
- 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 shall 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 must render their computer inaccessible.
- For Windows-based workstations, lock the system by pressing the Ctrl-Alt-Delete keys simultaneously, then click on “Lock Computer”.

Quick tip

How to Achieve Physical Security

- Be alert to your surroundings
- Do not leave secured doors open or unlocked
- Watch for tailgaters at badged entrances
- Question visitors or unfamiliar people without noticeable credentials
- Ensure data and documents are kept in secured locked down areas
- Ensure data and documents are physically destroyed before discarding
- Ensure the screensaver or monitor is locked before leaving desk

Laptop and Portable Device Security

Due to the small form factor and portability of laptops, tablets and smartphones extra security measures shall be taken.

- Protect devices with protective covers from physical damage.
- Wireless connections should be limited in use and securely connected following CJIS policy requirements.
- Maintain situational awareness when using electronic devices,
  - Would you wave $1500 cash at strangers?
- Never carry more information in your mobile device than needed.
- Don’t connect to unknown, unsecure wireless hotspots.
- Personal devices/computers from home shall not connect to the secured network without approval or policy enforcement.

Laptop and Portable Device Security

Common technology to help protect information to or on devices may include encryption (FIPS 140-2), Virtual Private Network (VPN) connections, Mobile Device Management (MDM) software, and Advanced Authentication (AA) methods.

Check with your agency TAC, LASO or IT support regarding specific extra security measures for laptop and portable device CJIS requirements.

Lost or Stolen Computers

If your TLETS computer or your vehicle with a laptop or portable device is lost or stolen, it is imperative to notify your Local Agency Security Officer (LASO) or Terminal Agency Coordinator (TAC) immediately.

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

Additional Roles for IT Personnel

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

- Anti-virus, malicious code scans and definition updates
- Data Backup and storage – centralized or decentralized
- Timely application of system patches – part of configuration management
- Access control measures
- Network infrastructure protection measures

More information in the CJIS Security Policy Section 5.2 and Appendix G

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 process, transmit or store Criminal Justice Information.

Personnel Security

- The least amount of computer privilege to accomplish a work task at a system is provided for security reasons.
- Personnel are presented with a system use message upon entering a secured network to acknowledge acceptance of system use.
- Multiple personnel may perform similar tasks for separation of duties to promote a crosscheck of duties and limit security threats.

Data Classification

- Many personnel have regular access to confidential intelligence, investigative, and/or criminal history information as a part of their official duties. **This includes systems like Driver License, CCH, Secure CCH Website, Secure Sex Offender, TLETS, MBIS, FES, T-DEx and N-DEx, etc.**

- All personnel must clearly understand that any unauthorized access and/or dissemination of this confidential information is a clear violation of the CJIS Security Policy and, in some cases, a violation of state and federal law. **This includes searching yourself, other employees, family, etc.**

- Data derived from DPS systems shall be treated as confidential and have restricted use.

- CJIS Information should be marked “For Official Use Only” or “Confidential”.

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 you have stored for private use, believing it to be safe.

A hacker's objective is to break into your computer and steal information. Implementing security in multiple ways makes intrusion more difficult to a hacker. Hackers prefer easy access and often will forgo systems where access is not easy to obtain. Apply as many security layers as possible between your system and the hacker.

Don't let your system be an easy target.

Security defense in layers.

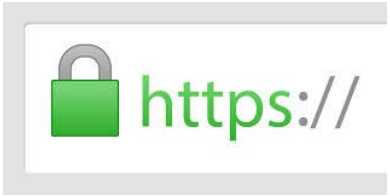
Secure Email

- CJI related data sent over email or internet sources must be encrypted before leaving the agency.
- Encryption method shall meet FIPS 140-2 level encryption.
- Check with your local IT support for methods utilized at the agency.

Securing Sensitive Data

Ways to protect your vital information

- Ensure the computer system is protected with a robust password.
- Ensure the computer is updated with patches (operating system and applications).
- Practice smart internet habits when performing financial transactions on-line. Be selective of sites you visit and check the security level of web pages requiring personal information.
- When entering personal information on a website, verify the website is encrypted. A lock should appear on the browser window signifying the website is encrypted.
- Another indication the website is secured is located in the address line in the browser window. Look for an address starting 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

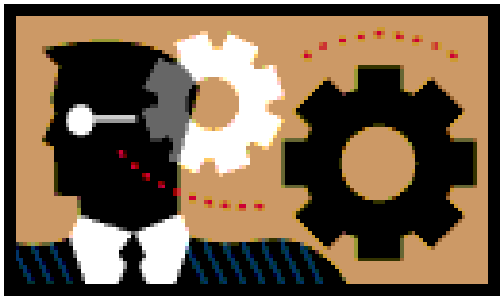
Natural and Unintentional Threats

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

Physically breaking systems

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" get them in where they're **NOT** supposed to be by using:

- Charm
- Intimidation
- Trickery

Hi, this is Joe from IT, we are moving email accounts today and need your password so your email is not deleted.

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 Scenario # 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 Scenario # 2:

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

Social Engineering

Social Engineering Scenario # 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

Defend 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 organizations 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 your password may have been compromised, 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 (has an Originating Identifying Number (ORI)) of such information and is being serviced by the accessing agency.

Sensitive Data Dissemination

- Only those individuals whose job duties include dissemination of confidential information will provide this information in response to authorized inquiries. A breach of this policy is grounds for disciplinary action, up to and including termination and a breach of the associated laws may result in criminal penalties.

- 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.

Do not use your authorized access for personal gain!

Sensitive Data Disposal

When no longer using disks, tapes, DVDs, CDs, USB drives, paper hard copies, print-outs, and other similar items, destroy them by shredding, burning, deguassing or physically breaking into undistinguishable pieces.

DO NOT PLACE SENSITIVE DATA IN TRASH CANS

Media Disposal

- Shred cross-cut best

- Burn

- Physically Destroy

Media Disposal for IT personnel

- For computer systems being repurposed the hard drives must be overwritten a minimum three times before reuse.

- Systems that are no longer usable or leaving the agency permanently, the media should be physically destroyed, the destruction witnessed and documented.

Summary

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

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

CJIS Security Office Contacts

CJIS Information Security Officer

Stephen 'Doc' Petty

(512) 424-7186

CJIS Technical Team Lead

Deborah Wright

(512) 424-7876

Technical Auditors

James Buggs (512) 424-7794	Chip Burleson (512) 424-7401	Jeannette Cardenas (512) 424-7910	Daniel Conte (512) 424-7137
Oswald Enriquez (512) 424-7914	James Gore (512) 424-7911	Linda Sims (512) 424-2937	Sonya Stell (512) 424-2450

Email to: security.committee@dps.texas.gov