



# 2016 Annual Cyber Security Awareness Training



# Applicability

- All Western Federal and Contract employees are required to complete annual Cyber Security Awareness Training (CSAT).
- North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) awareness training (CIPSAT) is also required, and is included in a separate module (starting on slide 47).

# Training Goals

- Ensure that everyone uses Western information and computing resources in a protective, effective, efficient, ethical, and lawful manner.
- Ensure that everyone agrees to the Rules of Behavior and uses Western equipment and accounts only for the authorized purposes.
- Test employees understanding of the material with a multiple choice test.

# Contents: Cyber Security Awareness Training (CSAT)

<b>Topic</b>	<b>Page</b>
• Applicability	2
• General computer and information use	6
• Responsibility and Accountability	9
• Using a Western Computer – Limited Personal Use	10
• Employee Access and Protection	13
• Password Management	14
• Using Email	15
• Local Administrator Accounts	16
• Portable and Removable Media	17
• Cell Phone Security	23
• Protecting sensitive information	24
• Social Engineering	29
• Identity Theft	37
• Malware	42
• Rules of Behavior and Acceptable Use Policy	43
• Further Reading	46

# Contents: CIP Security Awareness Training (CIPSAT)

<b>Topic</b>	<b>Page</b>
• NERC Critical Infrastructure Protection	47
• Key Terms	53
• Cyber Security Policies	55
• Physical Access Controls	56
• Electronic Access Controls	57
• Visitor Control Program	58
• Handling of BES Information	61
• Incident identification and notification	63
• Recovery Plans	64
• Response to Cyber Security Incidents	65
• Risks associated with interconnectivity	66
• Information Protection	68
• Change Control and Configuration Management	69
• Transient Cyber Assets	71
• OSEM Points of Contact	73
• Additional Training	74
• Cyber Security Points of Contact	75
• Addendum: Resources and Links	76

# General Computer and Information Use



# Definitions

- Cyber Security is concerned with protecting both information and information systems.
- Computing resources are any computer, programmable device, media, mobile device, server or network provided or supported by Western including Bulk Electric System (BES) Cyber Assets as defined by NERC.
- Western information is:
  - Programs and/or data stored on any storage media that is owned, leased, or maintained by Western.
  - Any Western information or data that has not been publically released and is stored or in transit on any device or electronic communication system (e.g., email).

# Why Cyber Security?

Loss of information or control of an information system could severely impact Western operations, national security and the safety and security of Western employees, our customers and the public.



**Responsibility and Accountability**

**All employees are  
responsible for protecting  
information from  
unauthorized access or  
modification.**

# Using a Western Computer

Using Western computers and information is one privilege of employment that comes with certain responsibilities:

- Use only approved and procured software to keep your system up to date and secure; request and obtain approval for any non-standard software.
- Once software has been properly assessed and approved by Cyber Security, follow Western approved acquisition processes
- Limited personal use of IT resources is allowed, but only as described in DOE Order 203.1
- There is no expectation of privacy; all Western systems are monitored.

# Using a Western Computer (cont.)

- Activate your screen lock when leaving your computer
- Take your badge with you or other security tokens with you whenever you leave your work station.
- Secure any sensitive documents or media
- Shut down your computer at the end of your day, unless instructed otherwise
- Do not write down or share your badge PIN
- Report a lost badge immediately
- Do not use your computer for illegal or inappropriate activity

# Misuse of Western Computers

Employees will not use Western computing resources to:

- View or download pornography
- Gamble on the internet
- Conduct private business/money-making ventures
- Load personal/unauthorized software or programs
- Make unauthorized configuration changes
- Play games during work time that is not during “fair use” or personal time

# Employee Access and Protection

- Access to Western information systems is based on identification, authentication, and access authorizations.
- This means that your username and password, or your badge and PIN, will allow access to files and programs you are authorized to use.
- Authorization is role based and the role is assigned by the Supervisor to match the responsibilities the individual will be assigned.
- Never share your badge PIN or your password with anyone, not even your supervisor or IT personnel.

# Password Management

## Passwords must contain:

- 15 characters at a minimum, when supported by the system
- At least one special character
- At least one uppercase letter
- At least one lowercase letter
- At least one number
- Do not use personal information, common phrases or entire dictionary words in your passwords
- Secure your password reminders and password reset questions
- Change your password regularly
- Never re-use passwords on different systems, such as using the same passwords at your home and at work
- Never share your password
- Securely store passwords physically or by encrypted methods such as approved password management software

# Email at Western

- Follow Western's terms of use for email, per the Rules of Behavior
- Do not use email to sell anything
- Do not send chain letters, jokes, offensive letters, mass email, unnecessary pictures
- Use care when using "reply all" to prevent sending unnecessary email traffic or messages to those without a need to know
- Avoid personal use of Western's email system
- Delete email from unknown senders
- Consider configuring Outlook to use Text Only instead of HTML
- If you suspect an email is spam, forward it to [spam@wapa.gov](mailto:spam@wapa.gov) to allow further research by cyber security

# Local Administrator Accounts

- Local administrator accounts are sometimes allowed if justified by business requirements
  - Must be approved in writing by a supervisor
  - Must be removed when no longer required
  - Approved software and updates must be installed by your IT/support staff or other approved users whenever technically feasible.
- If you have a local administrator account:
  - Never log in routinely with an administrator or local administrator account.
  - Do not browse the internet using an administrator or local administrator account.

# Portable and Removable Media



# What is Portable and Removable Media?

Western allows and supplies employees portable and removable media for official use, such as laptop computers, tablets, mobile phones, CDs, and thumb drives, with the appropriate review and approval from supervisors and cyber security.

Portable media pose a number of additional cyber risks, including loss, theft and added vulnerabilities from viruses or malware so have more rules and considerations.

# Examples of Portable and Removable Media

## Removable media include:

- Thumb drives, flash drives, sim cards
- CDs and DVDs
- External hard drives
- Music players (such as iPods)

## Mobile computing devices include:

- Cell phones and smartphones
- Laptops
- Tablets
- Wireless readers (such as Kindle and iPad)
- Other portable electronic devices (PEDs)
- NOTE – NERC CIP terminology also refers to these as transient devices



# Using and Protecting Portable and Removable Media

- Do not use removable media that has not been approved by Western. (contact your cyber security officer or supervisor regarding the approval process)
- When traveling with a Western laptop: insure that it has full disk encryption installed, do not leave unattended, connect via VPN from outside Western.
- Keep personal and work media separate – never connect personal media at work or vice versa
- Never connect an unknown drive – such as those found in the parking lot or received from a vendor at a conference
- Do not charge personal devices through your Western computer; use an outlet or power strip
- Verify any unknown, nonWestern device or media with cyber security before use
- Do not attach removable media from a low security system to a medium or high security system (and visa versa).

# Using and Protecting Portable and Removable Media (cont.)

- Store portable and removable media according to the appropriate security classification in Western-approved storage containers or areas
- Label all removable media with appropriate category. Examples are:
  - BES Cyber System Information (BCSI) – Controlled Distribution – Official Use Only (for BCSI under Exemption 7E & 7F);
  - Official Use Only – Authorization Required Before Distribution (for non-BCSI security information under Exemption 7E & 7F);
  - Official Use Only (for Exemption 3) or;
  - PII – Official Use Only (for Exemption 2)  
Follow Western’s policy for sanitizing, purging, discarding, and destroying removable media
- Destroy classified removable media in accordance with its classification level
- Never insert removable media with unknown content into your computer

# Using and Protecting Portable and Removable Media (cont.)

- All Western employees must immediately report any lost or stolen Western devices or personal devices that contain Western information. Report to one or more of the following: Western IT Call Center, Cyber Security, Office of Security and Emergency Management, your supervisor.
- Sensitive information must never be stored on portable media unless approved in writing by a manager and must be encrypted.
- Western reserves the right to erase any Western device or device that has Western information on it, even a personal cell phone.

# Cell Phone Security

For both personally owned and work (Western owned) phones:

- Secure your phone physically
- Secure your phone with a PIN
- Use anti-virus on your phone
- Never store Western documents or photograph Western information on your personal phone
- Report a lost or stolen work phone immediately
- Never charge or tether your personal phone by connecting to any Western system. Charge your phone by connecting directly to a power source such as a power strip or electric outlet.
- Never charge or tether your Western phone by connecting to any Non-Western system.
- Please consult with your Cyber Security representative to obtain guidance regarding installation of operating system updates (iOS, Android, etc.) on a Western-owned phone when adequate Wi-Fi or Internet access is not available to perform the update.

# Protecting Sensitive Information



# What is Sensitive Information?

Sensitive information must be protected from unauthorized disclosure.

Sensitive information includes:

- Personally Identifiable Information (PII)
- Official Use Only (OUO)
- Information related to BES Cyber Assets & Systems, such as BES Cyber System Information (BCSI) (covered in the CIPSAT training module)

Refer to WAPA Policy 471.1 on Identifying and Protecting Official Use Only Information

Refer to WAPA Order 471.3 Information Control Order

No sensitive information can be stored on portable or mobile devices and media without management approval and must be encrypted. Contact your cyber security officer for more information)

# What is PII?

Personally Identifiable Information, or PII, is information about an individual maintained by an agency which can be used to distinguish or trace an individual's identity including but not limited to:

- Name (when combined with other identifying information)
- social security number
- date and place of birth
- mother's maiden name
- biometric records
- education
- financial transactions
- medical history
- criminal or employment history



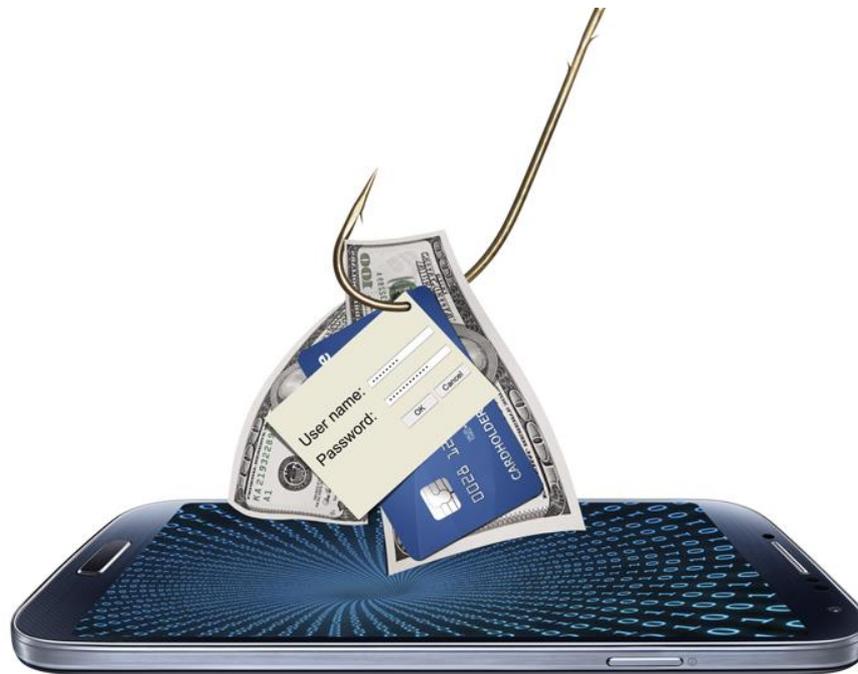
# Handling and protecting PII and other sensitive information

- Personally Identifiable Information (PII) that is stored or saved electronically must always be encrypted when technically feasible.
- Remote access to PII requires Multi Factor Authentication (MFA) such as a password AND a physical token such as a Personal Identity Verification (PIV) badge (per HSPD-12 ), not just a password.
- Any email with PII must be encrypted.
- Practice situational awareness and operational security (OPSEC). If you see something, say something – such as sensitive information physically out in the open, sensitive logical information that is improperly classified/stored/transmitted, an unrecognized person in the area, something unusual on your computer, or any other situations potentially impacting the security of Western information.

# OUO Information(continued)

- Information marked as Official Use Only (OUO) is unclassified information that could be used to damage Western, if not protected.
- Users must never place OUO data on any non-Western personal devices.
- OUO data must be encrypted when stored on portable media (“data at rest”) or electronically transmitted (“data in transit”).

# Social Engineering and Other Cyber Threats



# Social Engineering

Social engineering uses various methods of contact and trust building in order to elicit an action or divulging of information that can be used for malicious purposes such as entry to a building or performing cyber-attacks.

Social engineering takes many forms and methods:

- Phone calls from unavailable numbers, or posing as a known vendor or trusted party, who ask about your name, position, contact information, organization, co-worker information, or projects you are involved with in order to obtain more information about you and Western for misuse.
- Phishing emails that are crafted in such a way to entice you into clicking on malicious links or providing more information
- Social Networks (Facebook, Twitter, LinkedIn for example) and other online forums and email lists that may open you up to contacts looking to “friend” “follow” or “link” with you for the purpose of building trust that can later be misused, such as using your contact information for messaging, phone calls, and emails mentioned above.

# What is Phishing?

Phishing attacks use email, pop-ups, or malicious websites to solicit personal information by posing as a trustworthy organization. For example, an attacker may send email seemingly from a reputable credit card company or financial institution that requests account information, often suggesting that there is a problem. When users respond with the requested information, attackers can use it to gain access to the accounts.

# What is Phishing (cont.)

Phishing attacks may appear to come from other types of organizations, such as charities. Attackers often take advantage of current events, money concerns, or certain times of the year, for example:

- natural disasters (e.g., Hurricane Sandy, Indonesian tsunami)
- epidemics and health scares (e.g., H1N1)
- economic concerns (e.g., IRS scams)
- major political elections
- Holidays
- Money winnings,
- Job related benefits such as pay retirement information, pay increases or bonuses
- Anything that can elicit an emotional response

# Prevent Phishing Attacks

## 1. Limit your exposure

- Don't sign up for third-party email lists or to receive vendor information, or use a separate personal email address.

## 2. Treat all email with caution

- Be suspicious if it was unsolicited, seeks an urgent or emotional response, is poorly worded, or contains links to internet sites that you do not recognize
- If you think the email is safe, consider manually going the website instead of using a link in the email.
- Consider configuring your Outlook to open all messages as text only

## 3. Contact the sender's organization using a known phone number independent of what was provided to confirm the message's validity.

## 4. Never give out organizational, personal, or financial information to anyone by email.

# What is Spear Phishing?

Spear phishing is a more sophisticated phishing attack that appears to come from inside your organization or trusted source.

Spear phishing targets particular individuals, groups of people, or organizations.

To protect against spear phishing:

- Be wary of suspicious emails that use your name and/or appear to come from inside your organization or a related organization that seem out of character with normal communication.
- Call the sender to confirm the message's validity
- Forward any suspected spear phishing email to cyber security and then delete it.

# What is Whaling?

Whaling is a type of phishing attack that targets senior-level or high-risk personnel. Whaling:

- Uses personalized information: Name, title, official email address, sender names from personal contact lists
- Is an individualized, believable message
- Exploits relevant issues or topics

To protect against whaling:

- Be wary of emails that ask for sensitive information, contain unexpected attachments, or provide unconfirmed URL's or links
- Call the sender to confirm the message's validity
- Forward the whaling email to the Western IT Call Center (WITCC) or Cyber Security and then delete it

# What are Internet Hoaxes?

Hoaxes, often seen in chain letters, come in two types:

1. Attempts to trick or defraud by instructing users to delete a file necessary to the operating system or convincing users to send money or personal information
  2. Urban legends that warn users of a threat or claim to be notifying them of important or urgent information
- Hoaxes clog networks and slow down internet and email services, and sometimes be part of a distributed denial of service attack

To protect against internet hoaxes:

- Do not click on any links in a suspected hoax message
- Report suspicious messages or content immediately to Cyber Security and/or Western IT Call Center
- Don't forward suspected email hoaxes to co-workers
- Do not download any files related to a suspected internet hoax

# Protect against Identity Theft

Social Engineering can result not only in the disclosure of sensitive government information, but also in identity theft.

To protect your identity:

- Ask how information will be used before giving it out
- Pay attention to credit card and bank statements
- Avoid common names/dates for passwords and PINs
- Pick up postal mail promptly
- Shred personal documents
- Refrain from carrying your Social Security Card or Passport
- Order credit report at least annually and review

# If you are a victim of identity theft

- Contact credit reporting agencies
- Contact financial institutions to cancel accounts
- Monitor credit card and bank statements for unauthorized purchases
- Report the crime to local law enforcement

Learn more about Identity Theft:

<https://www.ftc.gov/news-events/media-resources/identity-theft-and-data-security>

# Dealing with suspicious email:

If you receive any suspected type of social engineering or spam message at Western, forward to the Western IT Call Center (WITCC),

[WesternITCallCenter@WAPA.GOV](mailto:WesternITCallCenter@WAPA.GOV)

and cc [spam@wapa.gov](mailto:spam@wapa.gov) and your Cyber Security Officer\*

(\*refer to the contacts list at the very end of this training)

# Thwart Social Engineering

- Always verify an unknown caller's identity and contact information before giving out any information. Take charge of the conversation and say you will call back. Limit the information provided.
- Alert cyber security of suspicious attempts to obtain information
- Do not participate in telephone surveys
- Do not give out personal information
- Do not give out computer or network information
- Do not follow any instructions from unverified personnel
- Document the interaction: Verify the identity of the individuals, write down their phone number, take detailed notes
- Contact Security and/or Western IT Call Center

# Thwart Social Engineering (cont.)

- Report any contact by foreign nationals
- Treat new connection requests with caution on social networks such as LinkedIn, Twitter, Facebook, online bulletin boards, email lists
- View email in plain text if possible
- Scan all attachments
- Delete emails from senders you do not know
- Don't forward infected or suspicious email or files to anyone but cyber security and [spam@wapa.gov](mailto:spam@wapa.gov) in order that they may be researched properly
- Refrain from accessing website links in email or popups

# If you suspect your computer is infected with malware

1. Disconnect the equipment from the Network/Internet.
2. Leave the equipment on; don't close or open new programs.
3. Write down any messages that appear on the monitor.
4. Note all events that occurred before and during the expected attack. (Did it come from an email link, email attachment, USB, web site, etc.?)
5. Report the incident immediately. Contact the Western IT Call Center (720-962-7111), your Cyber Security Officer\*, or your IT Manager. (\*refer to the contacts list at the very end of this training)

# Rules of Behavior



# Rules of Behavior – Acceptable Use Policies

The Rules of Behavior – Acceptable Use Policies outlines acceptable use by employees of the computer systems owned, provided, controlled or supported by Western, including servers and networks, computers and portable and storage devices and equipment.

**You must read Western’s Rules of Behavior:**

As part of the course test, you will be required to sign that you have read and understand the Rules of Behavior and accepted your responsibilities as a Western employee or contractor.

A link to the Rules of Behavior will be provided at the end of this training module.

# Rules of Behavior (cont.)

Noncompliance with the Rules of Behavior will constitute a security violation and will be reported to the management of the user and the Cyber Security Officer, and can result in short-term or permanent loss of access to computing systems. Serious violations may result in disciplinary action, and/or civil or criminal prosecution.

# Further Reading

- DOE O 203.1, Limited Personal Use of Government Office Equipment including Information Technology  
<https://www.directives.doe.gov/directives-documents/200-series/0203.1-BOrder>
- Rules of Behavior (refer to the Western internal web site)
- WAPA P 205.2D Cyber Security and Security Management Controls Policy
- Western Policy 200.3 Protecting Electronic Personally Identifiable Information
- Western Policy 471.1 Identifying and Protecting Official Use Only Information
- WAPA Order 471.3 Information Control Order



# 2016 NERC Critical Infrastructure Protection Training

# Applicability

- All Western Federal and Contract employees are required to complete annual North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) training
- Cyber Security Awareness Training is also required, and is included in a separate module that is part of this training (slides 1-46).

# NERC CIP training requirements

- Employees and contractors must take Western's annual Cyber Security Awareness Training (CSAT) and CIP Security Awareness Training (CIPSAT) which is comprised of these slides.
- Western will also provide, at least once each calendar quarter, awareness training that reinforces cyber security practices for the Western personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems. This quarterly awareness training may consist of Western articles, emails, posters, and presentations.

# NERC CIP training requirements (continued)

Included in this CIP Security Awareness Training are the following topics:

1. Cyber security policies
2. Physical access controls
3. Electronic access controls
4. The visitor control program
5. Handling of BES Cyber System Information and its storage
6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan
7. Recovery plans for BES Cyber Systems
8. Response to Cyber Security Incidents
9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with Removable Media.

# NERC CIP training requirements (continued)

Completion of this Cyber Security Awareness Training (CSAT) and CIP Security Awareness Training (CIPSAT) is required prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.

# Additional training goals

Ensure employees :

- Understand physical and electronic access controls to prevent NERC violations and protect BES Cyber Assets
- Properly handle and control information
- Develop awareness of the “rules of behavior” unique to accessing, operating, changing, and maintaining BES Cyber Assets

# Key terms

The following terms may be referenced in this training, and are important to understand for general CIP Security Awareness.

- Bulk Electric System (BES): As defined by the Regional Reliability Organization, the electrical generation resources, transmission lines, interconnections with neighboring systems, and associated equipment, generally operated at voltages of 100 kV or higher. Radial transmission facilities serving only load with one transmission source are generally not included in this definition.
- BES Cyber System: One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.
- BES Cyber Assets: A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, mis-operation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems

More information and additional terms may be referenced on the NERC web site. A link is provided in the Addendum: Resources and Links, located at the end of this training.

# Key terms (continued)

- Critical Assets: Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System
- Cyber Assets: Programmable electronic devices and communication networks including hardware, software, and data.
- Transient Cyber Assets: A Cyber Asset that (i) is capable of transmitting or transferring executable code, (ii) is not included in a BES Cyber System, (iii) is not a Protected Cyber Asset (PCA), and (iv) is directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless, including near field or Bluetooth communication) for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a PCA. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.
- Protected Cyber Asset (PCA)
- Physical Access Control System (PACS)
- Electronic Access Control and Monitoring (EACM)

# CIP Security Awareness Training Content:

## 1) Cyber security policies

Federal and contract employees with authorized logical access and/or authorized unescorted physical access to a BES Facility or BES Cyber Asset must be familiar with:

- Western Rules of Behavior
- Western Policy 205.2D Cyber Security and Security Management Controls Policy

Refer to the Resources and Links addendum, which provides links to this information.

# CIP Security Awareness Training Content:

## 2) Physical access controls

### Physical CIP Access:

1. All BES Cyber Assets are contained within a Physical Security Perimeters (PSP)
2. Only personnel with current authorization may enter the PSP without an escort. Never loan/share your badge with another individual. Report a lost or stolen badge immediately.
3. Tailgating (following, or allowing someone to follow) is prohibited, as NERC CIP requires that each individual be logged when passing through a PSP.
4. Authorized physical access to a PSP is controlled and monitored by means of an electronic Physical Access Control System (PACS). The PAC will grant access at medium impact facilities using a badge only. Access at a high impact facility will require both a badge and PIN.

# CIP Security Awareness Training Content:

## 2) Physical access controls

### Physical CIP Access:

5. In the event of a badge failure the individual requiring access must contact the Security Operations Center (SOC) with their name and assigned PACS PIN. The on duty Officer will confirm access is authorized in the PACS, and verify the name/PACS PIN combination is correct before granting access remotely over the PACS. Personnel shall contact the on duty Officer when departing.
6. In the event of a PACS system failure, a mechanical key-override process is instituted. Individuals requiring access to an override key must contact the SOC and verify identity by stating name and PIN. The on duty Officer confirms access is authorized in the PACS, and verifies that the name/PIN combination is correct before disclosing the key box combination.
7. For additional information, contact your regional OSEM representative, referred to on a later slide.

# CIP Security Awareness Training Content:

## 3) Electronic access controls

### Electronic CIP Access:

- NERC CIP Standards require that all logical access be logged when passing through a “Electronic Security Perimeter” when using a user ID and password
- Logical (electronic) access records must be kept at least 90 days.
- Logs must be kept longer if related to a reportable incident.

### Unless exempted in writing:

- DO NOT connect an outside digital device (transient cyber asset) to any asset within the electronic security perimeter. This includes devices such as: USB/thumb drives, CD/DVD, mobile phones, and laptops. Approval for use of these devices must be obtained in writing by the responsible manager, and should be assessed for risk by Cyber Security.
- DO NOT download software of any type or add or remove assets (unless approved via the CIP Change Control Process.
- DO NOT Use a BES Cyber Asset for personal use. These assets are for business mission use only.

# CIP Security Awareness Training Content

## 4) The visitor control program

Visitor Controls - When escorting visitors it is your responsibility to:

- Accompany any individual who does not have authorized, unescorted access privileges.
- Enter the area before the escorted person and leave the area after the escorted person.
- Maintain continuous line of sight or dedicated focus of the unauthorized person(s) while in the area.
- Limit the visitors to no more than five per escort. Ensure all individuals remain together in close proximity.
- Ensure visitor(s) sign the CIP area Visitor Log or, call the associated Security Operations Center (SOC) and report the required visitor information. When using a visitor log it is the escorts responsibility to ensure that visitors complete all fields listed in the visitor log. If calling the SOC it is the escorts responsibility to ensure information for all visitors is reported.

NOTE: CIP area Visitor Logs and SOP Daily Activity Reports (DAR) are collected and reviewed quarterly.



# CIP Security Awareness Training Content

## 4) The visitor control program (cont.)

Visitor Controls - When escorting visitors it is your responsibility to:

- Unauthorized individuals cannot remain in a CIP restricted area without an authorized escort present.
- It is your responsibility to know the logging procedures your Region uses and that your identity has been logged.
- Only those people with current authorization to enter the PSP can escort visitors or other unauthorized people.
- To escort someone means to keep them in your visual field of view when they are within the PSP and ensure that they do not harm the integrity of the critical cyber assets or the reliability of the Bulk Electric System.

NOTE: CIP area Visitor Logs and SOP Daily Activity Reports (DAR) are collected and reviewed quarterly.

# CIP Security Awareness Training Content:

## 5) Handling of BES Cyber System Information and its storage

### Information Protection:

Western computing resources are unclassified systems. Classified information may not be processed, entered, or stored on these computing resources.

Information is considered “classified” if it is Top Secret, Secret or confidential information, which requires safeguarding in the interest of national security as defined by Federal Authorities.

Users are responsible for protecting information from unauthorized access.

Users will not attempt to access any data or programs contained on any system for which they do not have authorization or explicit consent of the owner of the system.

# CIP Security Awareness Training Content:

## 5) Handling of BES Cyber System Information and its storage (continued)

Additional best practices to follow:

- Lock the workstation before you leave.
- Encrypt Official Use Only (OUO) and Personally Identifiable Information (PII) for electronic storage and/or transmission.
- Protect media from adverse conditions, such as heat and magnetic fields that can cause damage.
- Handle and process Engineering information as per Western O 471.3
- BES Cyber System Information contained on Transient Cyber Assets must be properly managed per Western policy and procedures. (Refer to the topics for Transient Cyber Assets, and Information Protection elsewhere in this training)

# CIP Security Awareness Training Content:

## 6) Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan

Be aware of how to identify incidents, as identified in the Western Incident Response Plan.

Incident identification and detection is described in Western's Cyber Security Incident Response Plan (CSIRP):

*"An incident is a violation or the threat of a violation of information security policies, acceptable use policies and/or other security policies. Examples of incidents include a Denial of Service (DoS) to a Western's web page, download and installation of malware through email or a web page, Western data loss not released through approved agency methods, the disclosure or compromise of Western credentials into a web site not managed by Western, or an unplanned disruption or the attempt of disruption to the BES by unauthorized personnel through a cyber security control. "*

Reference: [Western Cyber Security Incident Response Plan \(CSIRP\)](#).  
Refer to the resources and links addendum supplied with this training.

# CIP Security Awareness Training Content:

## 7) Recovery Plans for BES Cyber Systems

- Become familiar with the Recovery Plan for the assets in your area
- Know the roles you may be assigned for Recovery activity
- Insure that Recovery Plans are exercised periodically, at least annually
- Be familiar with any backup and restore procedures for assets in your area
- Backup and recovery of assets must be tested periodically, as defined in their recovery plan.
- Identify any lessons learned that are determined from Recovery tests, exercises, or real recovery activities.
- Update recovery plans to reflect lessons learned from recovery tests, exercises, or actual recoveries.

# CIP Security Awareness Training Content:

## 8) Response to Cyber Security Incidents

### Reporting Incidents:

Employees will report all incidents or attempts of anyone trying to gain unauthorized access to BES Cyber Assets or other computer resources to the proper authorities by contacting the Western IT Call Center (720-962-7111), your Cyber Security Officer\*, or your IT Manager.

Reference: Western Cyber Security Incident Response Plan (CSIRP).

Refer to the Resources and Links Addendum supplied with this training.

\*Refer to the Cyber Security Points of Contact addendum supplied with this training

# CIP Security Awareness Training Content:

## 9) Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with Removable Media.

Know the risks associated with systems interconnectivity:

- Risks associated with exposing connections outside the boundary, leading to loss of confidentiality, integrity, and availability

Know the risks associated with transient cyber assets and removable media:

- Risk from exposure to malware
- Risks associated with loss or theft
- Risks associated with unencrypted information, leading to loss of confidentiality
- Risks associated with moving from a low security enclave to a higher security enclave

# CIP Security Awareness Training Content:

## **9) Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with Removable Media. (cont.)**

Any new BES Cyber System connections must be formally reviewed and approved by Cyber Security personnel and/or managers of those systems via the appropriate Change Control and Configuration Management Processes.

Changes to existing BES Cyber System connections must be formally reviewed and approved by Cyber Security personnel and/or managers of those systems via the appropriate Change Control and Configuration Management Processes .

# Information Protection and BCSI

- Information Protection Officers will manage classification and categorization decisions for information – only these Officers can designate information as BES Cyber System Information, or “BCSI”
- Physical protection of BCSI is required in unmanned facilities, such as substations
- Follow best practices in your office – lock computer, file or put away paper
- Access to information will be granted to roles, not individuals
- Encrypt BCSI information whenever technically feasible, both data at rest (files) and data in transit (email)
- Mobile devices will require additional protection
- A signed user agreement (currently under development) will be required for personal phones as well as work phones accessing Western information including email
- Become familiar with best practices for media sanitization and destruction of disposed assets containing information as described in WAPA O 471.3
- Consult with your Cyber Security Officer for additional information
- Reference Western’s Information Control Order WAPA O 471.3 (Refer to the addendum at the end of this training for links to Western Orders)

# Change Control and Configuration Management

- Additions or Changes to BES Cyber Systems must go through the Configuration Change Management Process
- The Change Control Process includes cyber security testing and baseline management
- The Change Control Process will require that a baseline be performed on all assets. This will include all High (Eq. Control centers) and Medium (eq. Substations) Impact Bulk Electric System (BES)
- Baseline elements required by Change Control Process are as follows:
  - Operating System or firmware of BES asset
  - Commercial or open source application software installed on BES asset
  - Custom software installed on BES asset
  - Logical network port accessible on BES asset
  - Security patches applied on BES asset

# Change Control and Configuration Management (cont.)

- The Change Control and Configuration Management Process will utilize Service Now for its workflow and tracking
- Prior to implementing any change in the production environment (additions, removals or changes), testing will need to be performed and documentation of the results will be maintained through the Change Control and Confirmation Management process.
- Any changes that affect the baseline elements will need to be processed through Change Control. For a change that deviates from the existing baseline configuration, the baseline configuration will need to be updated within 30 calendar days of completing the change.
- Every High Impact BES asset's baseline will be monitored at least once every 35 calendar days for changes.

# Transient Cyber Assets

**Per the NERC Glossary, a Transient Cyber Asset is defined as:** A Cyber Asset that (i) is capable of transmitting or transferring executable code, (ii) is not included in a BES Cyber System, (iii) is not a Protected Cyber Asset (PCA), and (iv) is directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless, including near field or Bluetooth communication) for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a PCA. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

In plain English terms, transient cyber assets includes such things as USB sticks, portable hard drives, CD/DVD media, or devices such as laptops and mobile phones. These devices have the capability to store and transfer files from one area to another, and thereby pose risks that must be mitigated.

# Transient Cyber Assets (Continued)

Transient Cyber Assets (otherwise known as mobile devices/mobile media) pose a risk to the BES environment if not properly managed.

Be aware that transient cyber assets have requirements for:

- Device authorization
- Software authorization
- Security patch management
- Malware prevention
- Unauthorized use
- Contact your cyber security officer and your supervisor for more information on procedures and best practice.

# Office of Security and Emergency Management (OSEM) points of contact

Location	Name	Phone	Email

# Additional Training

- In addition to the training contained in the annual Cyber Security Awareness Training (CSAT) and CIP Security Awareness Training (CIPSAT) contained in these training slides, additional training may be required based upon your position, role, job duties, and access to Western information, assets, or external (non-Western) facilities.
- Discuss with your supervisor any additional training that may be required for your position, job duties, and access.
- Training may be required for non-Western personnel who need to access Western facilities.



# Addendum: Resources and Links

- NERC CIP Standards: <http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx>
- NERC Glossary of terms:  
[http://www.nerc.com/files/glossary\\_of\\_terms.pdf](http://www.nerc.com/files/glossary_of_terms.pdf)
- Western Orders:  
(refer to the Western internal web page)
- Western Rules of Behavior – Acceptable Use Policies:  
(refer to the Western internal web page)
- Western Cyber Security Information:  
(refer to the Western internal web page)
- Cyber Security Incident Response Plan (CSIRP)  
(refer to the Western internal web page)