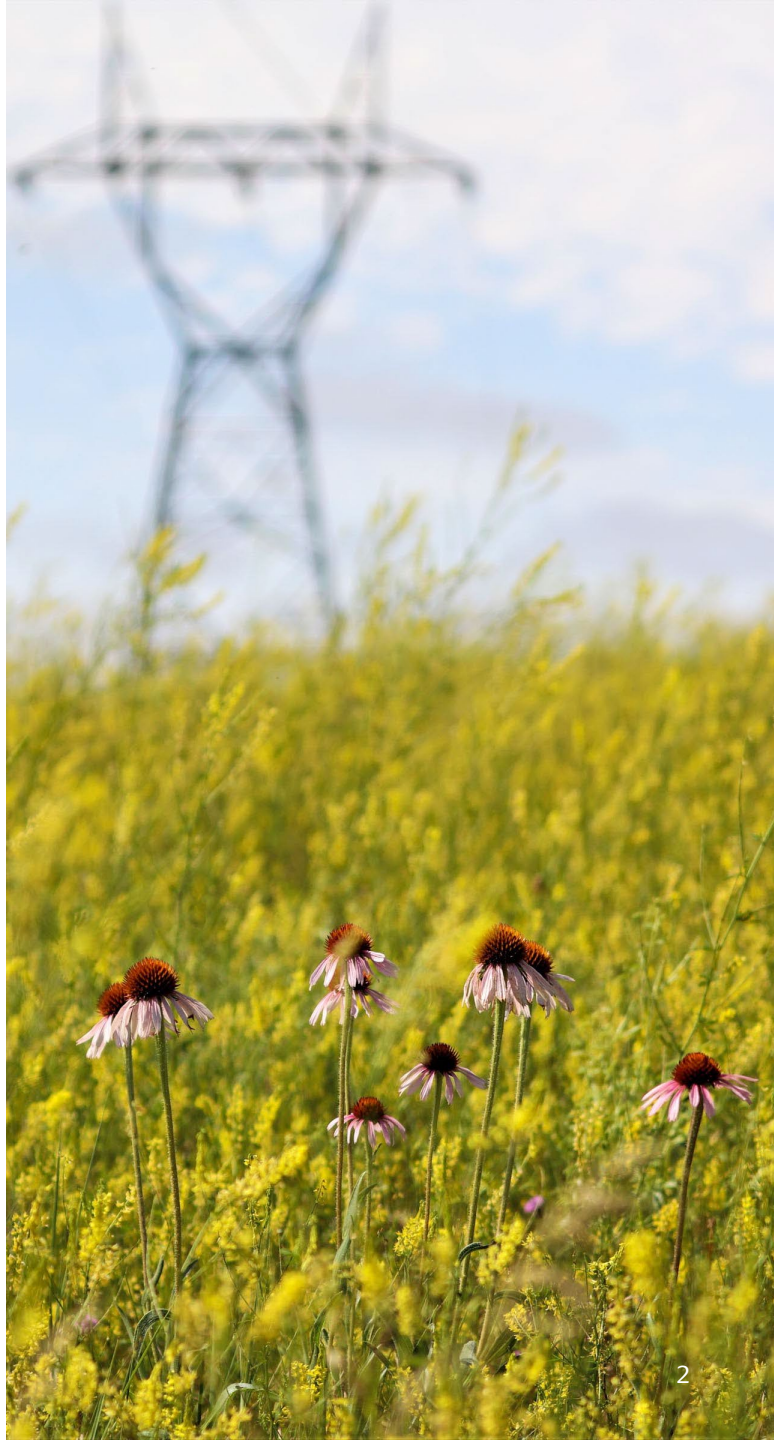
Western Area Power Administration

Annual NERC Critical Infrastructure Protection

Security Awareness Training

Table of Contents



Applicability

- All WAPA Federal and Contract employees with authorized electronic/logical/informational access and/or unescorted physical access to WAPA's defined North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Cyber Systems are required to complete this training annually.

- At least once each calendar quarter, Federal and Contract employees who have authorized electronic/logical or authorized unescorted physical access to Bulk Electric System (BES) Cyber will receive awareness training that reinforces cyber security practices.

- Quarterly awareness training may consist of WAPA publications, email, posters, and presentations.

CIP Security Awareness Training Campaign

- Annual CIP training for the current calendar year is released every March with a completion date of May 31.

- Dates reset each year. If you completed CIP cyber training prior to the start of the new campaign, you'll need to complete the updated training during the campaign period.

- Training is updated annually.

NERC CIP Training Requirements

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 (BCSI) 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

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

- This training is also required for information access, unless handling requirements are covered by other legal means (such as a non-disclosure agreement).

Additional Training Goals

Ensure employees:

- Understand physical and electronic/logical access controls to prevent NERC violations and protect BES Cyber Assets.
- Properly handling and control of 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 BES. 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.

Key Terms

- **Critical Assets**: Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the BES.

- **Cyber Assets**: Programmable electronic devices and communication networks including hardware, software, and data.

- **Transient Cyber Assets (TCA)**: 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 Electronic Security Perimeter (ESP) containing high or medium impact BES cyber systems, 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):** One or more Cyber Assets connected using a routable protocol within or on an ESP that is not part of the highest impact BES Cyber System within the same ESP. The impact rating of PCAs is equal to the highest rated BES Cyber System in the same ESP.

Key Terms

- **Physical Access Control System (PACS):** Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s) (PSP), exclusive of locally mounted hardware or devices at the PSP such as motion sensors, electronic lock control mechanisms, and badge readers.

- **Electronic Access Control and Monitoring (EACM):** Cyber Assets that perform electronic access control or electronic access monitoring of the ESP(s) or BES Cyber Systems. This includes Intermediate Systems.

- **Physical Security Perimeter (PSP):** The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled

- **Electronic Security Perimeter (ESP):** The logical border surrounding a network to which Critical Cyber Assets are connected and for which access is controlled.

Key Terms

- **External Routable Connectivity (ERC):** Direct user-initiated interactive access or a direct device-to-device connection to a low impact BES Cyber System(s) from a Cyber Asset outside the asset containing those low impact BES Cyber System(s) via a bi-directional routable protocol connection. Point-to-point communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions between Transmission station or substation assets containing low impact BES Cyber Systems are excluded from this definition.

Key Terms

- **BES Cyber System Information (BCSI):** Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System.

More information and additional terms may be referenced on the NERC web site. A link is provided in last slide located at the end of this training.

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:

- WAPA Rules of Behavior
- WAPA Policy 205.2H Cyber Security and Security Management
- WAPA Order 470.1i Safeguards and Security Program
- WAPA Order 471.3A Information Control Order

See the last slide for links to these resources.

2) Physical Access Controls

Physical CIP Access:

- All BES Cyber Systems are contained within a PSP.
- Only personnel with current authorization may enter the PSP without an escort. Never loan/share your badge or key with another individual. Report a lost or stolen badge or key immediately.
- Tailgating (following, or allowing someone to follow) is prohibited, as NERC CIP requires that each individual be logged when passing through a PSP.
- Authorized physical access to a PSP is controlled and monitored by means of an electronic PACS. The PACS is used to grant access at medium impact facilities using a badge only. Access at a high impact facility will require both a badge and PIN.
- If you do not know if you have authorized access to an area of the building, talk to your supervisor
- The PACS or a lock is used to grant access at low impact facilities. (Refer to next slide)

2) Physical Access Controls

Physical Security is afforded to all WAPA Low Impact BES Cyber Systems and physical access is based on need. At a minimum, the physical security afforded shall include at least one of the following, as deemed most appropriate by WAPA:

- The BES Cyber System is located within a locked building when not attended
- The BES Cyber System is located within a building with entrances which are alarmed through a PACS system or a SCADA system
- The BES Cyber System is located within a locked cabinet.
- Personnel entering a control building must notify system Operations of their entry and sign the substation logbook (both entry and exit)

2) Physical Access Controls

Physical CIP Access – Any Facility:

- 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.
- 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.
- For additional information, contact your regional OSEM representative.

3) Electronic/Logical Access Controls

- Electronic CIP Access
  - NERC CIP Standards require that all logical access be logged when passing through an ESP 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.

3) Electronic/Logical Access Controls

- Unless exempted in writing:
  - DO NOT connect an outside digital device (TCA or removable media) to any asset within the ESP. 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 Management Process.
  - DO NOT Use a BES Cyber Asset for personal use. These assets are for business mission use only.

Authorized TCA like laptops **must** connect to the WAPA GSS network for updates to anti-virus, Operating System, Applications, or other approved changes prior to connecting to CIP Low, Medium, or High impact BES Cyber Systems, EACMS, PACS, and/or PCA.

3) Electronic/Logical Access Controls

- WAPA does not allow vender remote access to any BES Cyber Systems to include their associated EACMS, PACS, and PCAs. Vendors will not be provided any ability to initiate authenticated remote access sessions for any high or medium impact (sans ERC) BES Cyber systems to include their associated EACMS, PACS, and PCAs.

- At no time will a vendor remote viewing session be established from within the ESP to systems outside the ESP.

3) Electronic/Logical Access Controls

WAPA will only utilize remote viewing for vendors through available online meeting technologies and sessions which will require the following meeting configurations prior to initiation:

- All connections that will require Vendor Remote Viewing sessions must be initiated through an Interactive Remote Server (IRA).
- The session is to be configured for shared screen functionality only.
- The session shall disable the ability to control applications, web browsers, or systems remotely.
- The session shall be configured to end meetings automatically.
- WAPA personnel will validate a BES Cyber System Information (BCSI) NDA is in place prior to the session.

4) The Visitor Control Program

Visitor Controls - When escorting visitors within a CIP PSP it is your responsibility to:

- Understand that only those people with current authorization to enter the PSP can escort visitors or other unauthorized individuals into the PSP.
- Continually escort any individual who does not have authorized, unescorted access.
- Enter the area before the escorted person and leave the area after the escorted person.
- Limit the visitors to no more than five per escort and keep visitors in close proximity.

4) The Visitor Control Program

Visitor Controls - When escorting visitors within a CIP PSP, it is your responsibility to:

- Conduct a proper handoff of escorting duties if you need to depart the area. This handoff must include:
  - Ensuring the new escort has authorized, unescorted privileges within the PSP
  - Briefing the escort on the visitors present, including names, orgs, purpose for entering the PSP, time entered, and how access into the PSP was logged
  - Verbal confirmation from the new escort that they understand they are assuming all escorting responsibilities and understand what those responsibilities entail
  - Notifying the visitors present of who is the new escort

Know the logging procedures your Region uses and log all visitors into a PSP

4) The Visitor Control Program

Visitor Controls - When escorting visitors within a CIP PSP, it is your responsibility to:

- Visitors must either sign the associated CIP area visitor log or call the associated SOC who records visitor information on a Daily Activity Report (DAR).
  - Recorded visitor information includes date and time of the initial entry and last exit, visitor name, and name of responsible host.
  - It is the responsibility of the escort to ensure that visitors complete all fields listed in the visitor log or all visitor information is reported to the SOC.

4) The Visitor Control Program

Visitor Controls - When escorting visitors within a CIP PSP, it is your responsibility to:

- Ensure no visitor harms the integrity of the Cyber Assets or interferes with the reliability of the BES
- Maintain continuous line of sight and positive control of the unauthorized person(s)
- Positive control is the ability to direct actions of the visitor

AT NO TIME SHALL ESCORTED VISITORS BE LEFT UNATTENDED

*NOTE: CIP area Visitor Logs and DARs are collected and reviewed quarterly.

5) Handling of BCSI and It's Storage

BCSI Protection:

- Users are responsible for protecting BCSI from unauthorized access.
  - If you do not know if something is BCSI or not, please contact your regional information system security officer or cyber security compliance support person for your region.
- Users will not attempt to access any BCSI or programs contained on any system for which they do not have authorization or explicit consent of the owner of the system.
- Before sharing BCSI, verify the recipient is authorized to receive BCSI.

5) Handling of BCSI and It's Storage

Additional practices to follow to protect BCSI:

- Lock the workstation before you leave.
- Encrypt Controlled Unclassified Information (CUI), BCSI, and Personally Identifiable Information (PII) for electronic storage and/or transmission.
- Protect media from adverse environmental conditions, such as heat and magnetic fields that can cause damage.
- Handle and process Engineering information as per WAPA O 471.3A (Information Control Order)
- BCSI contained on TCA must be properly managed per WAPA policy and procedures. (Refer to the topics for TCAs, and Information Protection elsewhere in this training)

5) Handling of BCSI and It's Storage

- 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.

5) Handling of BCSI and It's Storage

Information Protection and BCSI:

- Information Protection Officers (IPOs) will manage classification and categorization decisions for information.
- Classification Officials are designated by the IPOs and designate information as BCSI. The Classification Officials are members of the IT Cyber Security Information Assurance Group and the IT Cybersecurity Compliance Support Group.
- Physical protection of CUI including BCSI, is required in unmanned facilities, such as substations.
- Follow best practices in your office – lock computer, file, or put away paper.

5) Handling of BCSI and It's Storage

Information Protection and BCSI (Cont.):

- Encrypt BCSI and other CUI information whenever technically feasible, both data at rest (files) and data in transit (email).
- Mobile devices require additional protection. A signed user agreement is required for work phones as well as personal phones accessing WAPA information including email.
- Become familiar with best practices for media sanitization and destruction of disposed assets containing information as described in WAPA O 471.3A.
- Consult with your ISSO for additional information.
- Reference WAPA's Information Control Order WAPA O 471.3A (Links on last slide)

5) Handling of BCSI and It's Storage

BCSI Updates – Approved Locations and Procedures:

- Approved Systems designated for storing BCSI
  - Maximo - Asset Management System
  - Engineering Design Drive – Access Controlled CIP File Storage
  - Cybersecurity Compliance Support SharePoint Site
  - ASPEN Relay Database
  - See the WAPA O471.3A Information Control Order (links on last slide)
- To get access, your supervisor must request your entitlements to these sites using WAYS (where you can filter available roles using "CIP")

5) Handling of BCSI and It's Storage

BCSI Updates – Approved Locations and Procedures (Cont.):

- Example WAYS BCSI Related Access Entitlements:
  - CIP Aspen
  - CIP Maximo
  - CIP SharePoint <insert specific library names>
  - CIP Engineering Drawings <insert region>
- WAYS requires your supervisor to include a statement of your need for access with the request.
- Access authorization should be verified before sharing BCSI.

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 WAPA Cyber Security Incident Response Plan (CSIRP).
- Report suspected cyber security incidents immediately to WITCC or your Information System Security Officer (ISSO).
- Incident identification and detection is described in WAPA's CSIRP as:
- *"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 WAPA's web page, download and installation of malware through email or a web page, WAPA data loss not released through approved agency methods, the disclosure or compromise of WAPA credentials into a web site not managed by WAPA, or an unplanned disruption or the attempt of disruption to the BES by unauthorized personnel through a cyber security control. "*

Reference: WAPA CSIRP (link on last slide)

7) Recovery Plans for BES Cyber Systems

- Become familiar with the Recovery Plan for the assets in your area.
- Know the roles assigned to you for Recovery activity.
- Ensure that Recovery Plans are exercised and reviewed within 12 calendar months, no later than 15 calendar months.
- 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.
- Document any lessons learned, update the recovery plan based on lessons learned, and notify personnel with a defined role of the changes **within 90 days** of the exercise/recovery. **If there are no lessons learned, document there were none.**
- If a defined role or technology changes, plans must be updated, and notifications need to occur **within 60 days**

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 WAPA IT Call Center (720-962-7111), your Cyber Security Officer, your supervisor, or regional IT VP.

Reference: WAPA CSIRP

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

Know the risks associated with systems interconnectivity:

- Exposing connections outside the ESP for BES Cyber Systems leading to loss of confidentiality, integrity, and availability.

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

Know the risks associated with TCAs and removable media:

- Exposure to malware.
- Loss or theft.
- Unintentionally unencrypted information, leading to loss of confidentiality.
- Moving removable media from a non-CIP cyber asset to a low, medium, or high impact cyber asset (and vice versa).
- Moving a TCA from a low impact security zone to a medium or high impact security zone.

10) Change Control and Configuration Management

- Additions or changes to BES Cyber Systems must be approved via the Configuration Change Management Process.
- The change control process includes cyber security testing and baseline management.
- The change control process
  requires the establishment of a baseline configuration for all High (Control Center) and Medium (substation) BES Cyber Systems and their BES Cyber Assets and PCAs, EACMS, and PACS.

10) Change Control and Configuration Management

- The Change Control and Configuration Management Process will utilize Service Now (WAYS) (IT assets) and Maximo (maintenance assets) for its workflow and tracking.
- Prior to implementing any change in the production environment (additions, removals, or changes), testing will need to be preformed 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.

10) Change Control and Configuration Management

Baseline elements required by the 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

10) Change Control and Configuration Management

- Every high impact BES asset's baseline will be monitored at least once every 35 calendar days for changes.
- All high and medium impact cyber assets prior to a change must verify the identify of the software source and the integrity of the software obtained. Examples include downloading from secure vendor websites, secure packages, verification of hashes, and packages signed with a certificate.

11) TCAs and Removable Media

TCA:

Per the NERC Glossary, a TCA is defined as a Cyber Asset that:

- is capable of transmitting or transferring executable code;
- is not included in a BES Cyber System;
- is not a PCA; and
- 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.

11) TCAs and Removable Media

- Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.
- In plain English terms, TCAs includes devices such as laptops, mobile phones, storage devices, or any other device that can execute programs. These devices have the capability to store and transfer files from one area to another, and thereby pose risks that must be mitigated.

11) TCAs and Removable Media

TCAs pose a risk to the BES environment if not properly managed. Be aware that TCAs 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.

11) TCAs and Removable Media

Prior to connecting any TCA to any identified BES Cyber System, you must:

- Be authorized in the WAYS system to possess and use Removable Media on a BES Cyber Asset.
- Ensure the TCA has been connected to the WAPA business network so the latest software patches, antimalware software, and signature patterns can be updated.
  - This should be done prior to travelling to a site where there is no network connectivity.
- Verify the most current antivirus signature file has been downloaded to the device (if supported).
- Execute a scan on the TCA with the current antivirus signature file

Under no circumstances should the TCA be connected if malware has been detected.

11) TCAs and Removable Media

Removable Media:

Prior to connecting any Removable Media to any identified BES Cyber System, you must:

- Be authorized in the WAYS system to possess and use Removable Media on a BES Cyber Asset.
- Execute a scan on the removable media with the current antivirus signature file using the most current antimalware software and signature file(s).
- Do NOT execute the scan on the BES Cyber Asset. This must be done separately on another cyber asset.
- Document the results of the scan. Examples of evidence can include a screenshot of a successful clean scan.

Under no circumstances should the removable media be connected to a BES Cyber Asset if malware has been detected.

11) TCAs and Removable Media

Removable Media:

Prior to connecting any Removable Media to any identified BES Cyber System, you must:

- Be authorized in the WAYS system to possess and use Removable Media on a BES Cyber Asset.
- Execute a scan on the removable media with the current antivirus signature file using the most current antimalware software and signature file(s).
- Do NOT execute the scan on the BES Cyber Asset. This must be done separately on another cyber asset.
- Document the results of the scan. Examples of evidence can include a screenshot of a successful clean scan.

Under no circumstances should the removable media be connected to a BES Cyber Asset if malware has been detected.

11) TCAs and Removable Media

Removable Media/TCA:

Additional Information:

- Vendors are not authorized to connect TCA or removable media to any WAPA-owned BES Cyber Systems and associated EACMs, PACS, and PCAs
- In the event of an emergency, authorization must be obtained from regional cybersecurity personnel
- Refer to the WAPA-wide plan for TCA/RM for the appropriate process to follow

Additional Training

- In addition to the CIPSAT, additional training may be required based upon your position, role, job duties, and access to WAPA information, assets, or external (non-WAPA) 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-WAPA personnel who need to access WAPA facilities or locations containing BES Cyber Systems (low, medium, or high impact).

Resources and Links

- WAPA Rules of Behavior and Acceptable Use Policy
- NERC CIP Standards
- NERC Glossary of terms
- WAPA Order 470.1i Safeguards and Security Program
- WAPA O 471.3A Information Control Order
- WAPA Policy 205.2H Cyber Security and Security Management
- WAPA Cyber Security Incident Response Plan
- Memo listing BCSI Repositories (restricted access)
- NERC Reliability Compliance Homepage on MyWAPA

Resources and Links

If you have questions about NERC Reliability Compliance

- See the WAPA NERC Reliability Compliance homepage on MyWAPA
- Contact your Reliability Compliance Manager (contacts at the above link)