



Cyber Security Training Handbook

Table of Contents

Introduction	2
2.1.1 Cyber Security Policies.....	5
2.1.2 Physical Access Controls	6
2.1.4 Visitor Access Control Program	8
2.1.3 Electronic Access Controls.....	9
2.1.5 BES Cyber System Information	14
2.1.6 and 2.1.8 Cyber Security Incidents	16
2.1.7 Recovery Plans for BES Cyber Systems	18
2.1.9 Risks with Interconnectivity and Interoperability	19
CIP Training Form for Contractors	20
Attachment 1: NERC Glossary of Terms	23
Attachment 2: Transmission Methods of BCSI	26



Introduction

Questions?	If you have any questions about compliance with the NERC CIP requirements, contact CIP administration at 563-333-8118 or cipadministration@midamerican.com
Handbook for contractors	<p>This handbook is applicable to personnel with access to certain facilities and cyber systems.</p> <p>Contractors will, at all times, undertake and perform the work subject to the provisions of CIP programs for the North American Electric Reliability Corporation (NERC) requirements.</p>
NERC CIP requirements	NERC has cyber security standards focused on ensuring the reliability of the Bulk Electric System (BES). This comprehensive set of critical infrastructure protection (CIP) requirements is aimed at protecting the Bulk Electric System from malicious cyber attacks. This handbook applies to the version of the standards that are mandatory and enforceable.
Penalties for noncompliance	<p>Compliance with cyber security policies and procedures is mandatory. The penalties for noncompliance are severe – as much as \$1.6 million a day per violation.</p> <p>Failure to comply is subject to action appropriate to the severity of the violation, up to and including termination and/or possible criminal prosecution.</p>
Topics to be covered	The topics covered in this training are required by standard CIP-004, requirement R2. Depending on your work assignment, all topics may not apply to you. Additional training is provided to some resources for operational excellence.
Operational excellence	<p>Some practices may exceed what is required by the standards.</p> <ul style="list-style-type: none">• Practices may exceed the standards for in-scope Cyber Assets.• Practices may be applied to Cyber Assets that are not in scope.
Applicable facilities	<p>Applicable facilities include:</p> <ul style="list-style-type: none">• control facilities that control substations, generating stations and transmission lines connected to the Bulk Electric System• generating facilities, substations and transmission lines that provide direct support to the Bulk Electric System.

Continued on next page



Introduction, Continued

Cyber applicable systems

The CIP standards identify cyber applicable systems for the applicable facilities.

The CIP standards list applicable systems that must meet the requirements. The applicable systems vary depending on the requirement. Applicable systems may include BES Cyber Systems and/or their associated systems and/or other Cyber Assets. A CIP applicable system may be one Cyber Asset.

CIP compliance program documentation identifies the specific applicable systems by requirement.

Security controls are based on several factors

The CIP standards are not “one size fits all.” The level of cyber and physical security controls is based on many factors. In some cases, the security controls are used for operational excellence, even if not required by CIP standards.

Factor	Variables
Impact level	<ul style="list-style-type: none">• High• Medium• Low
Control Center	<ul style="list-style-type: none">• Control Center or not Control Center
Type of applicable system or Cyber Asset	<ul style="list-style-type: none">• Bulk Electric System (BES) Cyber Systems• Physical Access Control Systems• Electronic Access Control or Monitoring Systems• Protected Cyber Asset• Transient Cyber Asset
Connectivity	<ul style="list-style-type: none">• Locally connected to other devices using routable or nonroutable or not connected• Externally accessible by routable, dial up or not accessible externally
User access	<ul style="list-style-type: none">• Interactive• Remote• Individual or shared accounts

Definitions

The NERC standards use some terms that you may not be familiar with. Some of these terms have official definitions included in the NERC Glossary of Terms. Several of these definitions are included in an attachment at the back of this document. The company’s official CIP documents contain supplemental information about these definitions.

Continued on next page



Introduction, Continued

Background checks and training before authorization

Before access to certain systems can be authorized, the NERC standards require:

- background checks (including identity verification and seven-year criminal background checks)
- training

The company requires background checks and provides this training to other individuals for operational excellence.



2.1.1 Cyber Security Policies

Cyber security policy and other documents

Cyber security policies address the following topics.

For high impact and medium impact BES Cyber Systems:

- personnel and training (CIP-004)
- Electronic Security Perimeters (CIP-005) including Interactive Remote Access
- physical security (CIP-006)
- system security management (CIP-007)
- incident reporting and response planning (CIP-008)
- recovery plans (CIP-009)
- configuration change management, vulnerability assessments and Transient Cyber Assets (CIP-010)
- information protection (CIP-011)
- declaring and responding to CIP Exceptional Circumstances

For assets identified in CIP-002 containing low impact BES Cyber Systems:

- cyber security awareness
- physical security controls
- inbound and outbound electronic access controls
- Cyber Security Incident response
- Transient Cyber Assets and Removable Media malicious code risk mitigation
- vendor electronic remote access security controls
- declaring and responding to CIP Exceptional Circumstances

The cyber security policy documents are listed in Cyber Security Policies and Senior Manager Identification. Important concepts from these policies are covered throughout this handbook.

Contact cipadministration@midamerican.com for a copy of any of the documents referenced in this handbook.

Declaring and responding to CIP Exceptional Circumstances

During emergencies, all efforts should be made to meet the CIP requirements using normal processes. Very few requirements allow for CIP Exceptional Circumstances, and then only for very specific situations involving safety or reliability.



2.1.2 Physical Access Controls

Access control The company restricts physical access to all applicable systems. Physical access controls requirements vary by applicable system. Access may be restricted using one or more of the following:

- personal identity verification system, with authentication through access cards, PIN or biometric devices
- personnel responsible for controlling physical access who are located on-site or at a monitoring station
- monitoring by systems, tamper tape or personnel
- locks

Multiple levels of access control may be used in combination at some locations.

High impact areas and Physical Security Perimeters High impact areas or locations are areas that contain high impact BES Cyber Assets, as well as their associated Electronic Access Control or Monitoring Systems and Protected Cyber Assets. Access is controlled at the physical borders surrounding these areas, which are called Physical Security Perimeters.

These high impact areas require two controls. Some other areas use two controls for operational excellence.

Compromised physical access controls If access controls to a controlled physical area are compromised due to malfunction or damage, it must be monitored until repairs are made. In no situation can an entry point be left or blocked open and left unattended.

If you become aware of a problem with a technical or procedural control for a CIP controlled area, contact the physical security alarm monitoring group at 515-242-4097, option 3, immediately.

When two controls are required At high-impact Physical Security Perimeters, you must always authenticate with both controls (such as an access card and PIN). Contact management immediately if you are unable to obtain access with both controls of the personal identity verification system. You will have to follow an alternative process for two controls or be treated as a visitor who is escorted.

Continued on next page



2.1.2 Physical Access Controls, Continued

Reporting unauthorized access	Unauthorized CIP access should be reported to the physical security alarm monitoring group immediately. This could include someone who has “tailgated” into the area, if the person is not authorized.
--------------------------------------	--

Logging	Entry into controlled areas must be logged. Logging can be done electronically, through the use of a card or hand reader, or manually on paper logs.
----------------	---

No tailgating!	Never allow another person to tailgate behind you into a high-impact PSP, even if you know the person is authorized for access into the area. Don’t assume the beep of a card reader indicates successful authentication. The CIP standards require dual authentication and logging of every person who accesses a high-impact PSP.
-----------------------	---



2.1.4 Visitor Access Control Program

Escorting visitors

The company has a visitor access control program at its facilities. Some areas subject to the CIP standards have additional visitor requirements.

A visitor is someone who requires access to the area but has not met the requirements of authorized personnel.

Requirements for escorting visitors include:

- A physical access log is maintained to track all visitors requesting access. If an area has a visitor log, it must be filled out.
 - Authorized personnel must continuously escort visitors within the controlled area.
 - Visitors must be continually within sight of the escort.
 - If the escort must leave the room where visitors are working, the escorting duties must be handed off to another authorized individual.
 - The escort can escort more than one visitor if the visitors remain within sight and activities can be monitored.
-

Visitor/escort log

It is the responsibility of the escort to ensure completion of the visitor/escort log. This includes:

- name of visitor
 - company/relationship of visitor
 - the individual point of contact responsible for the visitor
 - initial date and entry time in
 - last exit date and time out
-



2.1.3 Electronic Access Controls

Overview

The CIP standards include many controls to protect applicable systems when there is electronic access.

These controls are included in cyber security policies identified earlier in this training, including:

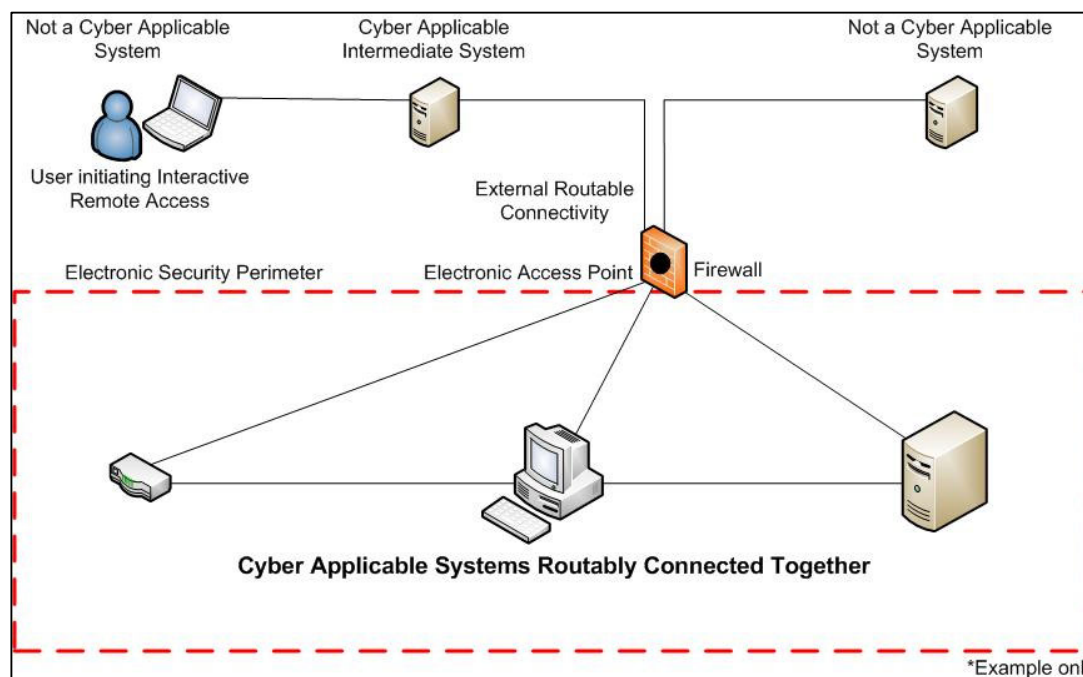
- Electronic Security Perimeters (CIP-005)
- systems security management (CIP-007)
- change management and vulnerability assessment (CIP-010)

Controls specific to ESPs

Electronic Security Perimeter

Some applicable Cyber Assets connected to a network with routable protocol must reside within an Electronic Security Perimeter, also known as an ESP.

- ESP is a concept. ESPs do not physically exist. They are virtual barriers preventing unauthorized electronic access to Cyber Assets.
- Cyber Assets within an ESP are accessible only through a defined Electronic Access Point for the ESP. An Electronic Access Point is the interface on a Cyber Asset that allows routable communication between Cyber Assets outside an ESP and Cyber Assets inside an ESP.



Continued on next page



2.1.3 Electronic Access Controls, Continued

Controls specific to ESPs, continued

External Routable Connectivity and permissions

- All External Routable Connectivity is through an identified Electronic Access Point. Access is denied by default.
- Inbound and outbound access permissions are required, including the reason for access.
- Applicable systems for Control Centers must have one or more methods for detecting known or suspicious malicious communications for both inbound and outbound communications.

Interactive Remote Access

- An Intermediate System is used so computers initiating Interactive Remote Access do not directly access applicable Cyber Assets. Encryption that terminates at an Intermediate System is used.

Vendor remote access management

The company must have one or more methods:

- for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access). The company uses a security information and event management system (SIEM) to meet this requirement.
- to disable active vendor remote access. This is done by manually logging off the user or terminating a web-based session.

Ports and services

Only logical network ports that have been determined to be needed should be enabled.

Physical input/output ports are protected. Protections could include:

- physical port covers or tamper tape.
- signage within the Physical Security Perimeter.
- disabling unneeded physical ports within the Cyber Asset's configuration.

Continued on next page



2.1.3 Electronic Access Controls, Continued

Account management

The following controls are used to manage electronic access into applicable systems:

- Authentication for interactive user access is enforced to ensure only authorized users can log on to applicable systems, where feasible.
 - Passwords for interactive user access must meet the following to meet the CIP requirements:
 - at least eight characters or the maximum supported by the Cyber Asset
 - minimum complexity of the lesser of:
 - three or more types of characters (uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric)
 - or
 - maximum complexity supported by the Cyber Asset

Note: Company network password policy requires 15 characters for operational excellence.
 - For password-only authentication for interactive user access, passwords must be changed annually.
 - Known default passwords must be changed if the Cyber Asset is capable.
 - When technically feasible, the number of unsuccessful authentication attempts must be limited or alerts are generated after the limit is reached.
 - All known enabled default or other generic account types must be identified and inventoried.
 - Access to shared accounts must be identified and authorized.
-

Controlling change

Baseline configurations

Baseline configurations must be developed for CIP applicable systems, including operating system or firmware, software, logical network accessible ports and applied security patches.

Changes to the baseline must be authorized and documented, and the baseline must be updated within 30 calendar days after the change is completed.

Continued on next page



2.1.3 Electronic Access Controls, Continued

Controlling change, continued

Change management

Prior to making changes, the company must determine what security controls could be impacted and then verify these controls were not affected after the change was made. The results must be documented.

For high impact BES Cyber Systems:

- Testing must be done in a testing environment or in a production environment in a manner that minimizes adverse effects.
- Monitoring must be done at least once every 35 calendar days for changes to the baseline configuration. Detected unauthorized changes must be investigated and documented.

Verifying software

Prior to making a change that deviates from an existing baseline, the following must be verified:

- identity of the software source
- integrity of the software obtained from the software source

Vulnerabilities

Patch management process

A patch management process is used for tracking, evaluating and installing cyber security patches for software or hardware cyber vulnerabilities for applicable Cyber Assets. Applicable patches must be applied within 35 calendar days of the evaluation or mitigation plans must be created or revised.

Vulnerability assessments

Medium impact BES Cyber Systems and associated Cyber Assets require a paper or active vulnerability assessment once every 15 calendar months.

High impact BES Cyber Systems and associated Cyber Assets require:

- a paper or active vulnerability assessment once every 15 calendar months.
- an active vulnerability assessment once every 36 calendar months.
- an active vulnerability assessment before adding new Cyber Assets to a production environment.

Continued on next page



2.1.3 Electronic Access Controls, Continued

Detecting, alerting and logging

Deter, detect or prevent

The company has methods to deter, detect or prevent malicious code.

Alerting and logging events

When possible, events of CIP applicable systems are logged, including:

- detected successful logins
- detected failed access attempts and failed login attempts
- detected malicious code

Alerts are generated at a minimum for:

- detected malicious code
- detected failure of event logging

Logs are retained 90 calendar days.

High impact areas require review of sample logs every 15 calendar days.



2.1.5 BES Cyber System Information

Overview	The information protection program includes identification, protection and the secure handling of BES Cyber System Information.
-----------------	---

BES Cyber System Information (BCSI)	The CIP information protection requirements apply to high and medium impact BES Cyber Systems, Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS).
--	--

The following information is considered BES Cyber System Information:

- shared passwords that provide direct access to applicable systems, including:
 - advanced level accounts in equipment that allow configuration settings to be changed or control an input/output device
 - administrator accounts
 - service (Windows or Unix) accounts
 - non-administrator accounts with permissions greater than view-only
 - community strings with more than read-only privileges
- security configuration information for applicable systems
- operational procedures or guides that contain security configuration information for applicable systems
- lists indicating critical assets or BES Cyber Systems, as required in standard CIP-002, and lists of other applicable systems
- backup files of applicable systems
- network topology or similar diagrams
- communication block diagrams for applicable systems
- schematic diagrams showing applicable systems that include logical configuration information
- schematics for access control and monitoring devices
- Physical Security Perimeter drawings
- protective relay and communication processor configuration/settings for applicable systems

Storage	BES Cyber System Information must be protected during storage, whether physical or electronic.
----------------	--

Physical media are considered protected if stored in a secured location to prevent unauthorized access.

Electronic information is considered protected if the drive, server or other location where the information resides has technical measures in place that, by default, deny access without proper user authorization and authentication.

Continued on next page



2.1.5 BES Cyber System Information, Continued

Handling	<p>BES Cyber System Information cannot be shared via:</p> <ul style="list-style-type: none">• unencrypted email to recipients external to Berkshire Hathaway Energy• social media, such as X, Facebook or LinkedIn• instant messaging: external• text messages <p>In addition, shared passwords to CIP applicable systems should not be shared through:</p> <ul style="list-style-type: none">• email within Berkshire Hathaway Energy (unless encrypted).• email or FTP: recipients external to Berkshire Hathaway Energy• third-party hosted secure electronic transmission• scanning• photography – hard copy or electronic• phone conference bridges or online meetings (internally or externally hosted)• faxing• printing at remote locations• mail: interoffice mail, USPS, FedEx, UPS <p>Reference: Attachment 2: Transmission Methods for BCSI</p>
Destruction and disposal	<p>BES Cyber System Information is considered confidential and is not in the public domain. Disposal of this information must be through secured document destruction methods.</p>
Reuse and disposal of a Cyber Asset	<p>Prior to the redeployment or disposal of a Cyber Asset that is part of an applicable system, the data storage media containing BES Cyber System Information will be erased or destroyed to prevent unauthorized retrieval of BES Cyber System Information.</p> <p>BES Cyber Asset redeployment or disposal is controlled by the change management process. The test guide attached to the change record in the asset's system of record documents the sanitization method(s) used and supporting evidence.</p> <p>Sanitization methods include clear, purge or destroy.</p>



2.1.6 and 2.1.8 Cyber Security Incidents

Definition of a Cyber Security Incident

Cyber Security Incidents are a malicious act or suspicious event that:

- For a high or medium impact BES Cyber System, compromises or attempts to compromise (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, or (3) an Electronic Access Control or Monitoring System; or
- Disrupts or attempts to disrupt the operation of a BES Cyber System.

Normal operational failures are not considered Cyber Security Incidents.

Identifying a Cyber Security Incident

A Cyber Security Incident may be identified through monitoring equipment and/or human observation.

If you suspect a Cyber Security Incident, the situation may require you to notify one or more of the following:

- CIP administration
- your supervisor
- the BHE service desk
- local law enforcement
- transmission operations/system control
- corporate security and resiliency
- global security operations center
- information technology
- field personnel who are incident responders

When in doubt, contact CIP administration at 563-333-8118, and they can help identify who should be notified.

The appropriate personnel determine:

- whether the event is considered a Cyber Security Incident.
 - whether the event has compromised or disrupted or an attempt to compromise or disrupt a BES Cyber Asset, Electronic Security Perimeter or Electronic Access Control or Monitoring System, making it a Reportable Cyber Security Incident.
 - what impact level of Cyber Assets were involved.
-

Continued on next page



2.1.6 and 2.1.8 Cyber Security Incidents, Continued

Reporting

NERC compliance, corporate security and resiliency, global security operations center, and transmission operations/system control work together to ensure notifications are made.

From determination, initial notifications are required:

- within one hour for a Reportable Cyber Security Incident involving medium and high impact BES Cyber Assets.
 - by end of next calendar day for attempts to compromise a system for medium and high impact.
-

Responding to a Cyber Security Incident

When responding to an event that could be a Cyber Security Incident, remember the following:

- Employee and public safety is the top priority.
 - System reliability is a priority. Take action to preserve the stability of the Bulk Electric System.
 - When a CIP applicable system meets the criteria to activate the CIP-009 recovery plan, preserve data for determining the cause of the Cyber Security Incident. Data preservation should not impede or restrict recovery.
-



2.1.7 Recovery Plans for BES Cyber Systems

- Recovery plans** The BES Cyber System Recovery Plan is activated when:
- a CIP applicable system is disrupted, compromised or failed
AND
 - information is required to successfully reconstruct a CIP applicable system to a functional state.

The following process is used.

Step	Action
Initial response by responding personnel	
1	Respond to notifications for device failures or security breaches.
2	Assess the situation to determine if: <ul style="list-style-type: none">• a CIP applicable system is disrupted, compromised or failed AND• information is required to successfully reconstruct a CIP applicable system to a functional state. <p>If no to either bullet, do not activate the recovery plan. If yes to both bullets, proceed to activate the recovery plan.</p>
Activation of recovery plan by responding personnel or change management approvers	
3	Contact the appropriate personnel for activation of the recovery plan. This might include: <ul style="list-style-type: none">• management for the affected departments• BHE service desk at 515-242-4357• CIP administration at 563-333-8118• global security operations on call at 515-281-2967• physical security alarm monitoring at 515-242-4097, option 3
4	Authorize the change record for recovery of the asset.
Data preservation by responding personnel	
5	Follow instructions from management as to whether to preserve data for post event analysis or continue with service restoration.



2.1.9 Risks with Interconnectivity and Interoperability

Overview	<p>What you do online has the potential to have significant impact because Cyber Assets may be interconnected, such as:</p> <ul style="list-style-type: none">• networked• temporarily connecting Removable Media, portable storage devices or Transient Cyber Assets
Networked Cyber Assets	<p>Controls for all CIP applicable systems (not just BES Cyber Assets) are covered in previous sections of this training, such as electronic access controls and cyber security policies.</p>
The risk of Removable Media or portable storage devices	<p>Connecting Removable Media or portable storage devices directly to company computing resources bypasses some of the security controls and can deliver malicious software into networks or result in loss of confidential information. The risks associated with connecting them to the network outweigh the benefits of their use.</p> <p>Only company-owned or authorized devices may be connected to company computing resources and networks. Personal devices, such as cellphones, SD cards and rewritable devices are prohibited, unless a documented exception has been granted.</p>
Risk of directly connecting to applicable systems	<p>A Transient Cyber Asset is one that is directly connected for 30 days or less to a: BES Cyber Asset; network within an Electronic Security Perimeter; or a Protected Cyber Asset.</p> <ul style="list-style-type: none">• Make sure wireless features are disabled to prevent the device from being a bridge to an outside network.• If it is necessary to connect a TCA to a medium or high impact applicable system, the CIP standard requires authorization.



CIP Training Form for Contractors

Instructions

- A copy of this document must be completed for every contractor employee who has authorized CIP access.
- The contractor employee must sign the contractor employee acknowledgement on the following page.
- The contractor employee must complete the 10-question assessment on the following pages.
Note: An 80 percent score is required to pass the assessment.
- Print, complete and send both pages:
 - mail them to CIP administration, MidAmerican Energy, PO Box 4350, Davenport, IA 52808-4350
 - OR
 - fax them to CIP administration, 563-333-8114
 - scan them and email them to cipadministration@midamerican.com

Continued on next page



CIP Training Form for Contractors, Continued

**To be
completed by
employee**

The undersigned acknowledges and agrees to comply with the NERC CIP programs, including the following:

- immediately reporting to their employer changes in employment status or need for CIP access.
- authorizing the employer to obtain and provide a compliant criminal history records check and identity confirmation.
- completing and following the CIP training.
- reviewing and observing security awareness materials.
- adhering to protected information program and handling procedures.

I personally agree with the provisions and terms of the CIP requirements. I personally have completed the assessment below. My agreement is evidenced by my signature below.

I HAVE READ THE FOREGOING AGREEMENT, UNDERSTAND ITS TERMS AND FREELY AND VOLUNTARILY SIGN THE SAME.

Signature by:	
Name printed:	
Company:	
Date:	

Assessment Please circle the correct answers.

#	Question
1	The critical infrastructure protection (CIP) requirements are mandatory and enforceable, with fines up to \$1.6 million a day. All efforts should be made to follow these standards, even during emergencies. A. True B. False
2	The CIP standards are not “one size fits all.” The level of security controls is based on several factors, including: impact level, type of applicable system, connectivity, whether at a control center and user access. A. True B. False
3	Physical Security Perimeters into high impact areas require just one physical access control. A. True B. False
4	It is acceptable to allow a visitor to be alone in a controlled area as long as you have logged the visitor. A. True B. False

Continued on next page

CIP Training Form for Contractors, Continued

Assessment,
continued

Please enter name: _____

#	Question
5	Passwords for interactive user access to applicable systems must meet which of the following requirement(s)? A. Have eight characters or maximum supported by the Cyber Asset to meet the CIP requirements, and 15 characters for company network password policy. B. Meet minimum complexity requirements (lesser of three or more types of characters or the maximum complexity supported by the Cyber Asset). C. Known default passwords must be changed if the Cyber Asset is capable. D. All of the above.
6	Which of the following is one of the acceptable methods for transmitting BES Cyber System Information? A. Unencrypted email to recipients external to the Berkshire Hathaway Energy network B. Voice conversation C. Social media, such as X (formerly Twitter), Facebook or LinkedIn D. External instant messaging
7	Which of the following is an example of a Cyber Security Incident? A. A normal operational failure of a substation relay. B. A bird watcher takes photographs outside a CIP facility. C. A backup control center facility gets broken into and computers are maliciously destroyed. D. An employee who is authorized for access into a PSP arrives at work without an access badge and is considered a visitor for the day
8	When a BES Cyber Asset fails and backup information is required to restore it, what important compliance step should be taken before the asset is recovered? A. If it doesn't impede recovery, preserve data to determine if the asset failed due to a Cyber Security Incident. B. Stop by the shop to obtain a new computer to replace the failed one. C. Call NERC to report the failure. D. There are no steps to take before fixing the equipment.
9	It is acceptable to charge a personal device, such as a cell phone, in a USB port on a company computer. A. True B. False
10	If you have questions about compliance with the NERC CIP requirements, who can you contact? A. Legal staff B. CIP administration C. Procurement D. The police



Attachment 1: NERC Glossary of Terms

Definitions

The following terms are defined in the NERC Glossary of Terms.

Term	Definition
BES Cyber Asset (BCA)	A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, 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.
BES Cyber System (BCS)	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 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.
Bulk Electric System	Unless modified by exclusion or inclusion lists, all Transmission Elements operated at 100 kV or higher and Real Power and Reactive Power resources connected at 100 kV or higher. This does not include facilities used in the local distribution of electric energy.
CIP Exceptional Circumstance (CEC)	A situation that involves or threatens to involve one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death; a natural disaster; civil unrest; an imminent or existing hardware, software, or equipment failure; a Cyber Security Incident requiring emergency assistance; a response by emergency services; the enactment of a mutual assistance agreement; or an impediment of large scale workforce availability.

Continued on next page



Attachment 1: NERC Glossary of Terms, Continued

Definitions, continued

Term	Definition
Cyber Security Incident (CSI)	A malicious act or suspicious event that: <ul style="list-style-type: none">• For a high or medium impact BES Cyber System, compromises or attempts to compromise (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, or (3) an Electronic Access Control or Monitoring System; or• Disrupts or attempts to disrupt the operation of a BES Cyber System.
Electronic Access Point (EAP)	A Cyber Asset interface on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.
Electronic Security Perimeter (ESP)	The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol.
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.
Protected Cyber Assets (PCA)	One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP.
Removable Media (RM)	<p>Storage media that:</p> <ol style="list-style-type: none">1. are not Cyber Assets,2. are capable of transferring executable code,3. can be used to store, copy, move, or access data, and4. are directly connected for 30 consecutive calendar days or less to a:<ul style="list-style-type: none">▪ BES Cyber Asset,▪ network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or▪ Protected Cyber Asset associated with high or medium impact BES Cyber Systems. <p>Examples of Removable Media include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.</p>

Continued on next page



Attachment 1: NERC Glossary of Terms, Continued

Definitions, continued

Term	Definition
Reportable Cyber Security Incident	<p>A Cyber Security Incident that compromised or disrupted:</p> <ul style="list-style-type: none">• A BES Cyber System that performs one or more reliability tasks of a functional entity;• An Electronic Security Perimeter of a high or medium impact BES Cyber System; or• An Electronic Access Control or Monitoring System of a high or medium impact BES Cyber System.
Transient Cyber Asset (TCA)	<p>A Cyber Asset that is:</p> <ol style="list-style-type: none">1. capable of transmitting or transferring executable code,2. not included in a BES Cyber System,3. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and4. 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:<ul style="list-style-type: none">▪ BES Cyber Asset,▪ network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or▪ PCA associated with high or medium impact BES Cyber Systems. <p>Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.</p>



Attachment 2: Transmission Methods of BCSI

Protecting BCSI during transit Use the table below to determine how to protect the security of BCSI during transit.

Shared passwords to applicable systems*	All other BES Cyber System Information	Transmission Method
PROHIBITED	PROHIBITED	Unencrypted email to recipients external to Berkshire Hathaway Energy
		Social media: such as X, Facebook, LinkedIn, Instagram, Snapchat
		Non BHE instant messaging service Examples: WhatsApp, Messenger, Slack
		Text messaging
PROHIBITED	ALLOWED	Unencrypted internal email within Berkshire Hathaway Energy
		Encrypted email, encrypted attachments to email or FTP: recipients external to Berkshire Hathaway Energy Note: Do not include the password in the same email. Deliver by phone or in an unrelated e-mail not mentioning the document name.
		Third-party hosted secure electronic transmission: Business partner secured Internet or intranet secure file transfer protocol (FTPS) sites with a secure protocol. When allowed, the information must be encrypted, must be on a specific IP address and have a password.
		Scanning (to a secured network location), including scanning documents to your email Inbox.
		Photography – hard copy or electronic
		Phone conference bridges or online meetings (internally or externally hosted) Examples: Microsoft Teams online meetings and/or conference bridges
		Facsimile transmission (faxing)
		Printing at remote locations
		Mail: interoffice mail, USPS, FedEx, UPS
ALLOWED	ALLOWED	Internal encrypted email or encrypted attachments within Berkshire Hathaway Energy Note: Do not include the password in the same email. Deliver by phone or in an unrelated e-mail not mentioning the document name.
		MEC hosted secure electronic transmission: encrypted MEC secured Internet or intranet secure file transfer protocol (FTPS) sites and a secure protocol. Note: Must be on a specific IP address and have a password.
		Hard copy
		Printing to printer in your office/work area
		Transmitted link to a secure drive, such as an email with a link to a document housed on a secured drive.
		Voice conversation
		Document management systems
		Instant messaging in Teams with someone within BHE

* This does not include view only shared passwords.