STANDARDS COMMITTEE
MIDWEST RELIABILITY ORGANIZATION
MRO Copyright 2007

STANDARD APPLICATION GUIDE

CIP-003-6 R2

CYBER SECURITY
SECURITY MANAGEMENT CONTROLS

VERSION 0.1

January 26, 2017

Authored by

Joe Peterson, *Minnesota Power*	Daniel Graham, *Basin Electric* Power Coop
Tim Anderson, *Dairyland Power Cooperative*	Ian King, *Xcel Energy*
Faisal Rahman, *Madison Gas & Electric*	David Seiler, *Great River Energy*

The MRO Subject Matter Expert Team is an industry stakeholder group which includes subject matter experts from MRO member organizations in various technical areas. Any materials, guidance, and views from stakeholder groups are meant to be helpful to industry participants; but should not be considered approved or endorsed by MRO staff or its board of directors unless specified.

Disclaimer

The Midwest Reliability Organization Standards Committee (MRO SC) is committed to providing training and non-binding guidance to industry stakeholders regarding existing and emerging Reliability Standards. Any materials, including presentations, were developed through the MRO SC by Subject Matter Experts (SME) from member organizations within the MRO Region.

The materials have been reviewed by MRO staff and provide reasonable application guidance for the standard addressed. Ultimately, demonstrating compliance depends on a number of factors including the precise language of the standard, the specific facts and circumstances, and quality of evidence.

These documents may be reproduced or distributed to any person or entity only in its entirety.

Acknowledgement

This publication was developed by a SME Team from MRO member organizations within the MRO footprint. The development of SME Teams is an ongoing effort to produce unified application guides for MRO and its registered entities.

The CIP-003-6 SME Team Chair, Joe Peterson (Minnesota Power), wishes to acknowledge and thank those who dedicated efforts and contributed significantly to this publication. The MRO, MRO SC, and their organizational affiliations include:

Midwest Reliability Organization

Richard Burt, Vice President
Risk Assessment, Mitigation and Standards

Russ Mountjoy, Manager
Standards, Registration and Certification

MRO Standards Committee

Robert Thompson, Chair
Xcel Energy

Dave Rudolph
Basin Electric Power Cooperative

Wayne Guttormson, Vice Chair
Saskatchewan Power

Joe Knight
Great River Energy

Mike Moltane
Dave Rudolph

Todd Komplin
WPPI Energy

Lori Frisk
Minnesota Power

Andrew Pusztai
American Transmission Company

Mark Buchholz
Western Area Power Administration

George Brown
Acciona Energy North America Co.

Table of Contents

Executive Summary

What: CIP 003-6 R2 includes requirements for cyber security awareness training, physical security controls, electronic access controls, and cyber security incident response.

Why: Responsible entities provide a standard minimum level of protection for low impact Bulk Electric System (BES) Cyber Systems.

When: Documentation of CIP-003-6 R2 plans and implementation of Attachment 1 Sections 1 and 4 becomes effective April 1, 2017. Implementation of Attachment 1 Sections 2 and 3 becomes effective September 1, 2018.

Who: The requirements apply to responsible entities with low impact BES Cyber Systems. Low impact BES Cyber Systems are all BES Cyber Systems that do not meet high or medium BES Cyber System criteria. BES includes 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.

How: There are many methods to apply these standards and responsible entities should choose the method most appropriate to their system. Below are a few examples of potential methods:

Cyber security awareness - computer-based training or posters

Physical security controls - badge accessed locked doors or padlocked fence

Electronic access controls - removal of all bidirectional communication or dial-up with access control

Cyber security incident response - tested existing cyber security incident response plan

Introduction

The intention of this guidance document is to assist entities with the application of North American Electric Reliability Corporation (NERC) Reliability Standard CIP-003-6 – Cyber Security – Security Management Controls. The guidance document is intended to be useful for entities with a wide range of CIP experience. Those entities without prior experience with CIP standards will benefit from the explanation of terms, clarification of requirements, identification of implementation dates, depiction of potential evidence, and recommendations to consider when developing programs. Entities more experienced with CIP standards will benefit from exposure to additional points of view and information regarding implementing plans and implementations from other standards.

NERC Reliability Standard CIP-003-6 (Under Revision)

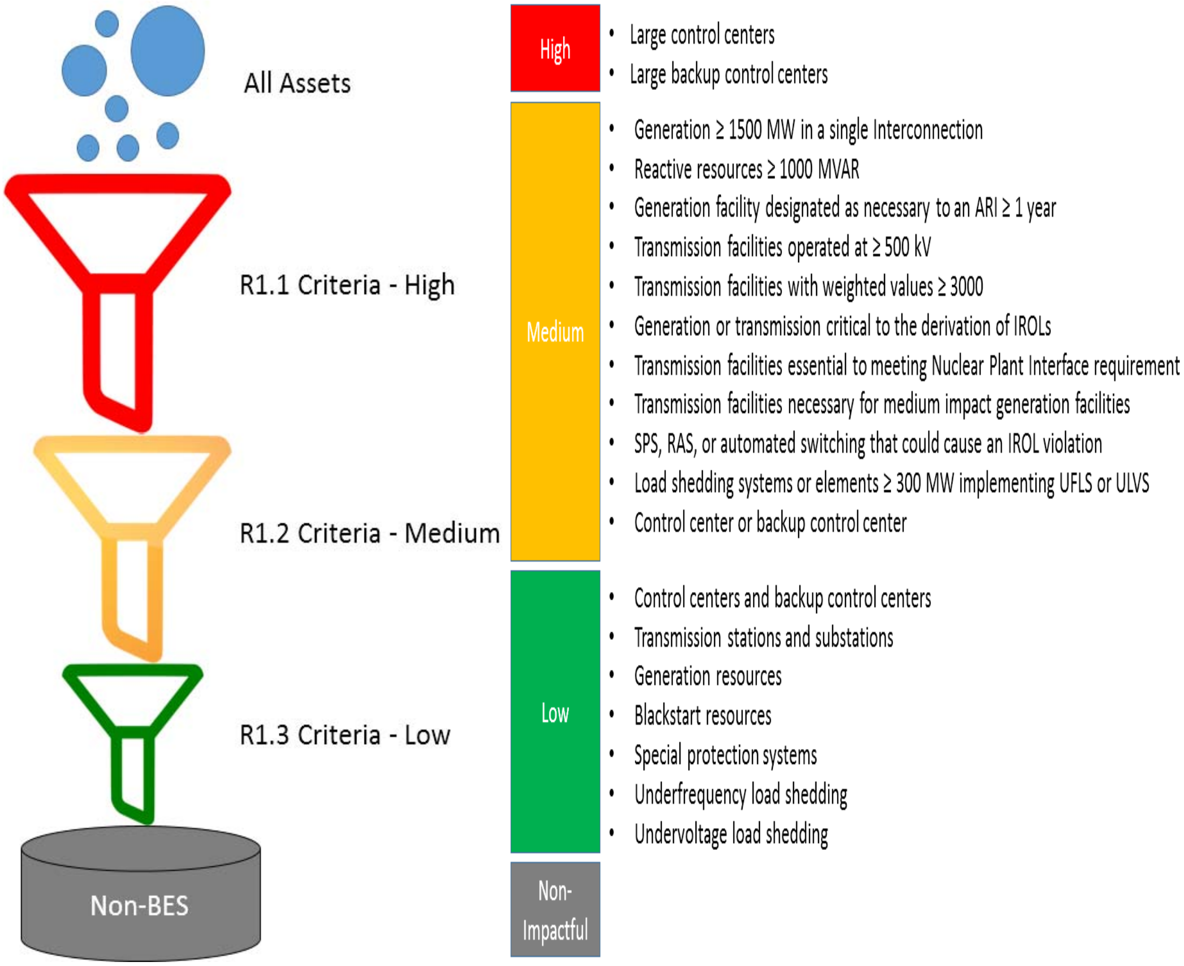
At the time that this document was under development, CIP-003-6 and related definitions were being revised by the Standards Drafting Team. Although it is possible that significant changes related to low impact BES Cyber Assets (BCA) will be adopted before the enforcement dates listed above (see “When:”), this document is written with the assumption that no new changes are in effect beyond what is required in CIP-003-6.

What is CIP?

Government agencies recognized a need to protect sectors which provide critical infrastructure that provide the essential services that support society. Energy is one of these sectors and includes the electric utilities. In order to provide a consistent minimum level of protection, governments enacted regulation for private industry to follow. The North American Electric Reliability Corporation (NERC) was chosen to act as the Electric Reliability Organization (ERO) and chartered to develop standards specifying requirements that entities are required to meet. Midwest Reliability Organization (MRO) and the other Regional Entities are assigned to monitor and enforce the Reliability Standards including the Critical Infrastructure Protection (CIP) standards for the electric industry.

Categories

The CIP standards split BES Cyber Systems into three impact ratings: high, medium, and low impact. BES Cyber Systems deemed high and medium impact have significantly greater requirements than low Impact BES Cyber Systems because the loss or misuse of high and medium BES Cyber Systems pose more risk to the Bulk Electric System. Each responsible entity is required to categorize its cyber systems by applying the criteria from CIP 002-5.1 BES Cyber System Classification to all of its BES Cyber Systems. The first set of criteria identifies the high impact BES Cyber Systems. The next set of criteria determines the list of medium impact BES Cyber Systems from the systems not categorized as high impact. The third filter classifies the remaining list as low impact BES Cyber Systems. All BES Cyber Systems that do not meet high or medium impact BES Cyber Systems criteria default to being low impact BES Cyber Systems. BES includes transmission elements operated at 100 kilovolt (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. Distribution level resources are only included if they are related to low impact BES Cyber Systems.


All Assets
R1.1 Criteria - High
R1.2 Criteria - Medium
R1.3 Criteria - Low
Non-BES
High
• Large control centers
• Large backup control centers
Medium
• Generation ≥ 1500 MW in a single Interconnection
• Reactive resources ≥ 1000 MVAR
• Generation facility designated as necessary to an ARI ≥ 1 year
• Transmission facilities operated at ≥ 500 kV
• Transmission facilities with weighted values ≥ 3000
• Generation or transmission critical to the derivation of IROLs
• Transmission facilities essential to meeting Nuclear Plant Interface requirement
• Transmission facilities necessary for medium impact generation facilities
• SPS, RAS, or automated switching that could cause an IROL violation
• Load shedding systems or elements ≥ 300 MW implementing UFLS or ULVS
• Control center or backup control center
Low
• Control centers and backup control centers
• Transmission stations and substations
• Generation resources
• Blackstart resources
• Special protection systems
• Underfrequency load shedding
• Undervoltage load shedding
Non-Impactful

The criterion for high and medium Impact BES Cyber Systems serve to identify those systems with the greatest potential impact to the BES. This inherently leads to the majority of the BES Cyber Systems being categorized as low impact. The low impact BES Cyber Systems category also encompasses systems with large variations, ranging from billion dollar plants to small substations. Due to the large range of facilities involved, entities are provided flexibility in how to comply with these standards. It is neither reasonable nor cost effective to apply the same security controls to the small substation as the billion dollar plant. Each entity should take measures appropriate for their situation and systems.

Applicable Requirements

The following requirements directly apply to low impact BES Cyber Systems: CIP 002-5.1 R1, CIP 002-5.1 R2, and CIP 003-6 R1-R4. The chart below lists these requirements and effective dates.

Standard	Requirement	Enforcement
CIP 002-5.1 R1.3	Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).	1-Jul-16
CIP 002-5.1 R2.1	Review the identifications in Requirement R1 and its parts (and update them if there are changes identified) at least once every 15 calendar months, even if it has no identified items in Requirement R1.	1-Jul-16
CIP 002-5.1 R2.2	Have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once every 15 calendar months, even if it has no identified items in Requirement R1.	1-Jul-16
CIP 003-6 R1.2	Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any: 1.2.1. Cyber security awareness; 1.2.2. Physical security controls; 1.2.3. Electronic access controls for Low Impact External Routable Connectivity (LERC) and Dial-up Connectivity; and 1.2.4. Cyber Security Incident response.	1-Apr-17
CIP 003-6 R2	Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1.	1-Apr-17
CIP 003-6 R2 Att 1, Section 1	Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).	1-Apr-17
CIP 003-6 R2 Att 1, Section 2	Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BES Cyber Systems within the asset and (2) the Low Impact BES Cyber System Electronic Access Points (LEAPs), if any.	1-Sep-18
CIP 003-6 R2 Att 1, Section 3	Electronic access controls: 3.1 For LERC, if any, implement a LEAP to permit only necessary inbound and outbound bi-directional routable protocol access; and 3.2 Implement authentication for all Dial-up Connectivity, if any, that provides access to low impact BES Cyber Systems, per Cyber Asset capability.	1-Sep-18
CIP 003-6 R2 Att 1, Section 4	Cyber Security Incident Response: have one or more Cyber Security Incident Response plan(s) either by asset or group of assets, which shall include: 4.1 Identification, classification, and response to Cyber Security Incidents 4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law 4.3 Identification of the roles and responsibilities for Cyber Security Incident response by group or individuals 4.4 Incident handling for Cyber Security Incidents 4.5 Testing the Cyber Security Incident response plan(s) at least every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security	1-Apr-17

	Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident 4.6 Updating the Cyber security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual incident.	
CIP 003-6 R3	Identify a CIP Senior Manager by name and document changes within 30 calendar days of the change.	1-Jul-16
CIP 003-6 R4	Implement a documented process to delegate authority, unless no delegations are used.	1-Jul-16

This guide focuses on CIP-003-6 R2 which contains the majority of the work load for low impact BES Cyber Systems. The plan(s) required for CIP-003-6 R2 cover four areas:

- cyber security awareness
- physical security controls
- electronic access controls
- cyber security incident response

Identifying Cyber Systems Requiring Protection

CIP Requirements Related to Low Impact BES Cyber Systems

A fundamental element of meeting the CIP-003-6 R2 requirement for protecting each low impact BES Cyber System is ensuring that all of the BES Cyber Systems are accounted for prior to applying controls. At some facilities it is most effective to simply protect all cyber systems. This may be the case for a small substation facility that has all BES Cyber Systems on a single network inside of a single building. At complex facilities, such as a large generating plant, it can be more effective to narrow the scope by eliminating cyber systems not related to the BES. By narrowing the scope of systems to protect, the physical and electronic security control efforts can be more focused and often simpler.

The CIP standard requirements allow entities a great deal of flexibility in this area, but offer little guidance. This flexibility can make the requirements seem incomplete or conflicting. Consider the following items from the CIP Standard requirements related to identifying the systems to protect:

- CIP-002-5.1 requires identification of assets containing low impact BES Cyber Systems
- CIP-003-6 requires protection of low impact BES Cyber Systems at identified assets
- CIP-002-5.1 and CIP-003-6 state that a discrete list of all low impact BES Cyber Systems is not required

It should be understood that the standard does not prohibit using an inventory list to identify low impact BCA or BES Cyber Systems. Maintaining an inventory of systems and configuration management for cyber assets is good security practice and is not discouraged by the NERC CIP Standards.

The CIP-003-6 requirements defining Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP) controls imply a requirement to identify certain Cyber Assets. All Cyber Assets that provide LEAP need to be identified and documented. Cyber Assets that have LERC communication through a LEAP will likely be identified by the LEAP access control policy.

Logically Separating Low Impact Functions from Higher Impact Cyber Systems

If a facility that can be logically split to isolate low impact from medium impact or high impact BES Cyber Systems, this should be considered. For guidance on the rules for defining facilities in this manner, please refer to the MRO Standards Committee CIP-002-5.1 Standard Application Guide.

General Approaches of Scoping to Include All Low Impact BES Cyber Systems

In order to apply the CIP-003-6 R2 controls, it is necessary to determine a set of the cyber systems at the asset that is known to include all low impact BES Cyber Systems. The entity may decide how widely or narrowly to define the set of cyber systems for each individual asset. Some approaches for selecting the cyber systems are:

- All Cyber Systems Approach: Protection is applied to all cyber systems at the asset
- Non-BES Cyber System Approach: Protection is applied to all cyber systems at the asset, except selected systems excluded by the criteria that they do not provide a BES Reliability Operating Service (BROS) and do not have a real-time operational impact
- Only BES Cyber Systems Approach: Protection is applied to those cyber systems identified as providing a real-time operation impact and provide a BROS

The use of cyber systems to group Cyber Assets is a tool for simplifying this consideration without having to fully specify or inventory every Cyber Asset. A cyber system can be used to generalize a whole set of Cyber Assets that have a commonality.

Examples of potential cyber system groupings include:

- Distributed Control System (DCS): a group of all Cyber Assets that make up a plant control system
- Programmable Logic Controller (PLC) System: a group of all PLCs and related Human Machine Interface (HMI) systems in a plant
- Coal Unloading System: a group of Cyber Assets that automate unloading of coal from rail cars
- Stand Alone Systems: a group of Cyber Assets that automate elements of the plant that are not able to impact the BROS functions performed by the plant (e.g., environmental or vibration monitoring systems that do not automatically interface to a plant DCS)
- Meters & Relays: a group of all electronic meters and protective relay devices
- Demand Response System: a collection of Cyber Assets that implement load control functions
- Business Systems: a group of all information technology that are not control system related

By thoughtfully defining cyber system groupings, the effort of limiting the scope of cyber systems is simplified to a smaller number of evaluations. The resultant evaluation will recognize a BES

Cyber System as one that has a real-time operations impact and provides a BES Reliability Operating Service (BROS). The definition of these criteria can be found in the CIP-002-5.1 Standard, and additional guidance can be found in the MRO Standards Committee CIP-002-5.1 Standard Application Guide. These evaluation criteria can be used to determine if certain cyber systems can be excluded from the program or help choose the most effective approach for applying protective measures.

It can help to identify devices that are not part of BES Cyber Systems if they would pose risk to security. Such cyber assets, if they are inside a control system network, can be moved to a different network and then eliminated by considering the BROS criteria. Examples:

- Identify non-BES Cyber Systems that are difficult to physically secure, such as: wireless systems, physically exposed systems, systems separated by significant distance or in a difficult to secure building
- Identify non-BES cyber systems that have a significant amount of external routable connectivity. All LERC must be controlled and managed, so simplification narrows the focus. It also reduces the exposure of other BES Cyber Systems from external exposure

Documentation of Work

Document the approach that is used at each asset and explain the major criteria used in this determination, for many assets, a simple statement or paragraph could explain appropriately. Alternatively, an entity may decide to maintain a direct inventory of BES Cyber Systems with a description of the criteria used to select each one. A list of cyber systems is not required evidence, but it is also not prohibited from being used as evidence.

Scoping Strategies

With the flexibility of different approaches, an entity can target the selection of cyber systems to ease implementation and management of the required electronic and physical access controls.

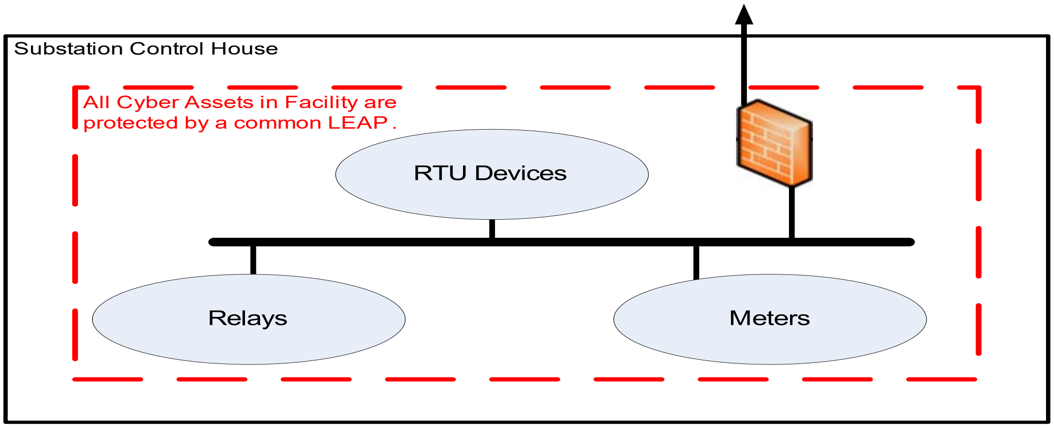
If a BES Cyber System can be defined within the boundaries of an existing network segment, the network segment is a good target for scoping a set of cyber systems for that asset. If the asset has an outlying building for a function that is not part of any BES service, then it is a good candidate for a cyber system that can be excluded from the program. With this in mind, sometimes it is best to make adjustments to the systems locations or connectivity to provide clear boundaries.

The following cases are examples. They demonstrate how the approaches might be used and the trade-offs. Different approaches could be used for each of these examples. Each entity will have to determine which approach to use.

CASE 1: A simple substation has all cyber systems connected to a common Local Area Network (LAN) and contained in a single control house.

- Approach Selected: All cyber systems
- LEAP will be the access point to the LAN

- The physical security perimeter will be the control house
- Discussion:
  - There is no real advantage to distinguishing cyber systems
  - All Cyber Assets on the LAN that have LERC will require the same LEAP policy
  - All Cyber Assets are contained in a physical building that can be secured.

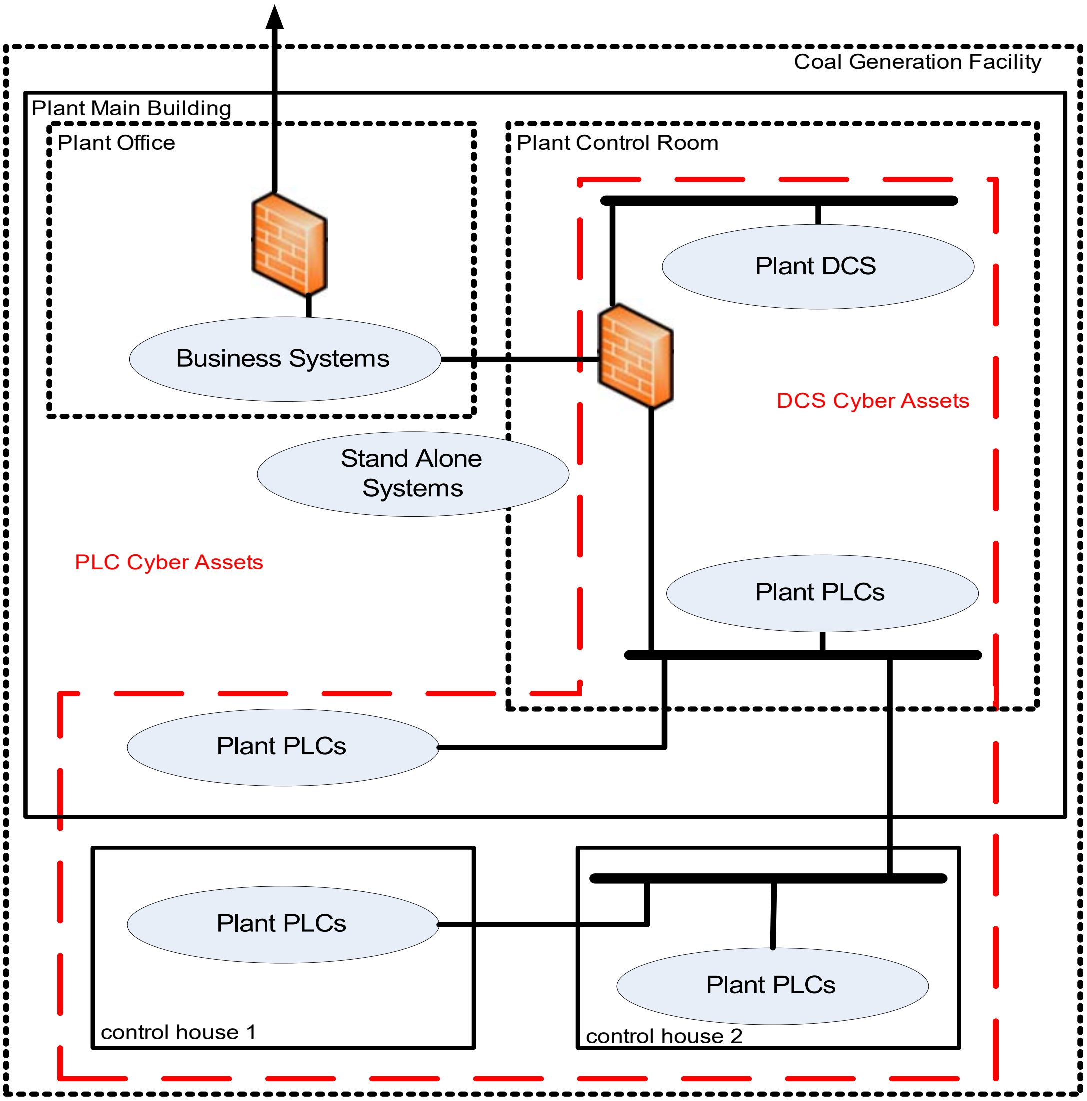

Substation Control House
All Cyber Assets in Facility are protected by a common LEAP.
RTU Devices
Relays
Meters

CASE 1: Substation

CASE 2: A coal generation facility with distinct networks for DCS, PLCs, stand-alone systems, and business systems. Systems are distributed across multiple buildings at the plant. Stand-alone systems are monitoring only and cannot impact the operation of the plant DCS.

- Approach Selected: Non-BES Cyber System selection
  - Identify non-BES business systems and stand-alone systems (devices that provide no BROS)
  - What remains is the DCS and PLC networks that contain all BES Cyber Systems
- LEAP will be the access point to the DCS and PLC networks
- The physical areas to secure will be the rooms in the buildings that contain the DCS and PLC systems
- Discussion:
  - By identifying all non-BES Cyber Systems (Business Systems and Stand Alone systems), it narrowed the scope to the Cyber Assets for the DCS and PLC systems that were segmented on their own networks. This is a smaller physical area to secure. This provides a boundary for a LEAP device that is focused on protecting BES Cyber Systems
  - Alternatively, an all cyber systems approach would have included many business systems that have a high need for external communications. All of these systems would need to be protected by a LEAP policy. This would lead to a complicated configuration to determine and maintain. This approach would distract attention from the protection of the BES Cyber Systems
  - Alternatively, a BES Cyber Systems Only approach could be used, defining both DCS and PLC as either separate cyber systems or a common cyber system. The evaluation would be different only in that it would identify all of the ways these

systems provide BROS. The resulting implementation would be identical to the Non-BES Cyber System identification approach

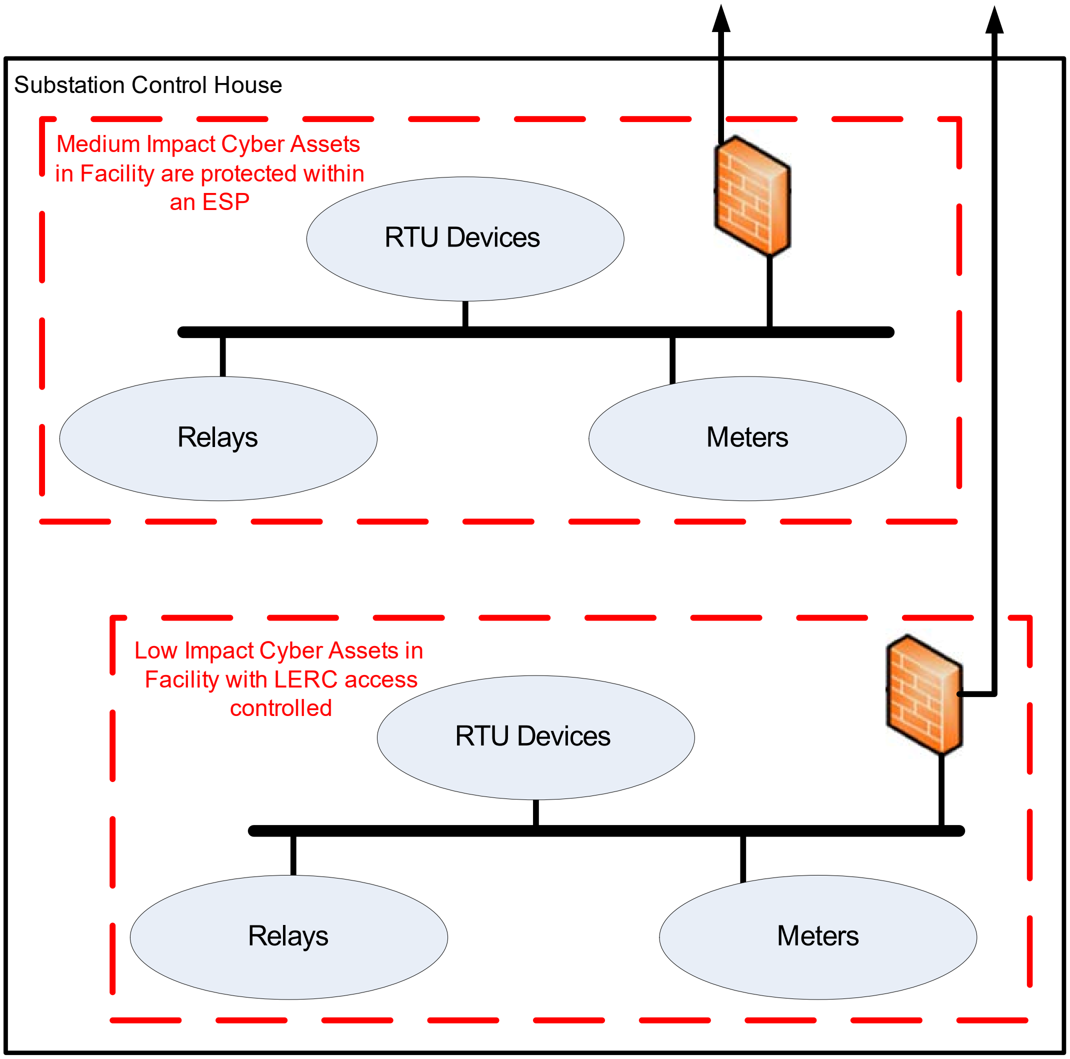


CASE 2: Coal Generation Facility

CASE 3: A single control house contains medium impact BES Cyber Systems and low impact BES Cyber Systems that can justifiably be separated into 2 Assets (or Facilities). Systems that meet medium impact criteria are in a defined Electronic Security Perimeter (ESP). Systems that meet low impact criteria are grouped in a separate network and access is controlled by a LEAP device.

- Approach Selected: BES Cyber Systems Only
- LEAP will be the access point to the LAN containing the low impact BCA
- The physical security perimeter for both Assets (Facilities) will be the substation control house
- Discussion:

- In this case the BROS criteria is already being directly applied to find the medium impact cyber assets, and so the same process can be continued to find the low impact BES Cyber Systems as well


Substation Control House
Medium Impact Cyber Assets in Facility are protected within an ESP
RTU Devices
Relays
Meters
Low Impact Cyber Assets in Facility with LERC access controlled
RTU Devices
Relays
Meters

CASE 3: Substation

Cyber Security Plan(s) (Requirement 2)

Entities must have a documented cyber security plan(s) that addresses cyber security awareness, physical security controls, electronic access controls for LERC and dial-up connectivity, and cyber security incident response. The plan(s) can address each topic in individual plans or collectively covered in a single plan. Additionally, entities can opt to:

- Leverage or add to the entity's existing security plan(s) (leverage medium or high impact cyber security plans)
- Create a stand-alone plan covering all BES assets containing low impact BES Cyber Systems

- Create individual documents per type of BES asset, individual BES asset, or grouping of BES assets

Each option has benefits and detriments. The table below lists some attributes: speed of implementation, standardization of design, scalability, flexibility of the plan, and expected buy in from facility personnel. These examples are not an all-inclusive list of attributes that may be useful to consider.

Table of Pros and Cons of Different Implementation Methods for Cyber Security Plans

	Existing plan	Stand-alone plan	Per asset plan
Speed	🔴	⊞	⭕
Standardization	⊞	🔴	⚫
Scalability	⭕	🔴	▦
Flexibility	⭕	▦	🔴
Buy in	⭕	⭕	🔴

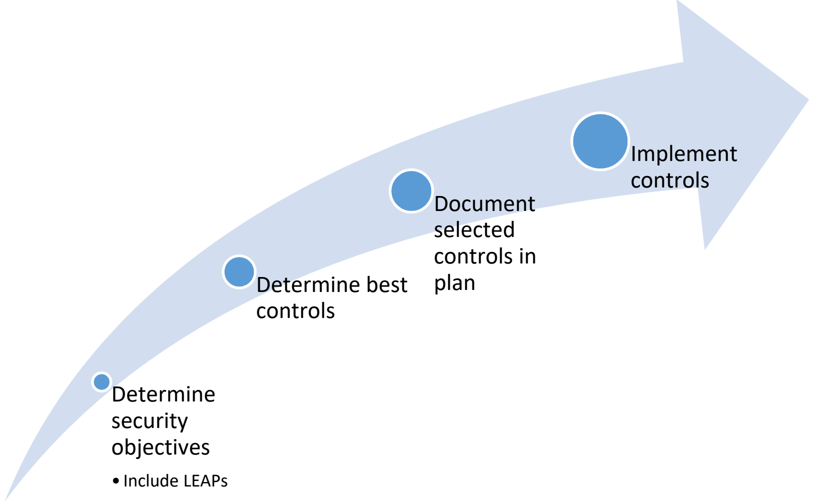
🔴	Very Good
⊞	Good
⭕	Average
▦	Poor
⚫	Very Poor

The chart shows pros and cons for methods of implementing security plans

Regardless of the method selected, it is advisable for entities to consider the following when developing the plan.

1. Determine the acceptable security objectives for protecting low impact BES Cyber Systems and physical location of LEAPs. Special consideration should be taken to ensure LEAPs that do not reside at the same physical location as the low impact BES asset are included in the plan if applicable. It can be helpful to document the philosophy used to determine requirements in the plan.
2. Determine which controls best meet the security requirements.
3. Document the selected controls in the plan including those for the low impact BES Cyber Systems and the LEAP protection. The focus of the requirement is the set of controls in place, not the access management processes (i.e. to whom or how access is granted).
4. Implement the new selected controls. Some controls may be controls that were implemented prior to the plan. It is cost effective and a good strategy to leverage existing controls when possible.

Security Plan Development Process

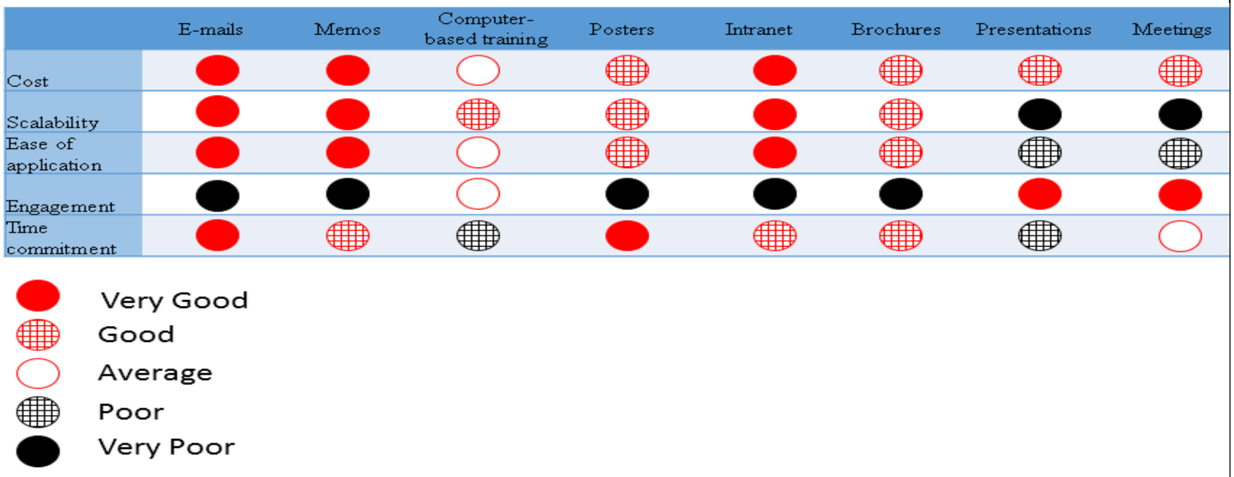

Determine security objectives
• Include LEAPs
Determine best controls
Document selected controls in plan
Implement controls

This diagram depicts the process of applying security controls

Cyber Security Awareness (Attachment 1, Section 1)

Responsible entities shall reinforce cyber security practices (which may include physical security practices) at least once every 15 months. These practices will align with the policy that entities created for CIP-003-6 R1. The policy and execution extends to external entities with access (joint ownership, visitors, contractors, etc.). Entities decide the awareness topics, how they will be conveyed, and schedules. For evidence, entities can produce the awareness material that was delivered and the delivery method(s) but do not need to maintain lists of recipients or track the reception of the awareness material by personnel. The requirement is best met by layering methods and applying them strategically. The following methods list of pros, cons, and recommended applications:

Pros and Cons of Cyber Security Awareness Methods



	E-mails	Memos	Computer-based training	Posters	Intranet	Brochures	Presentations	Meetings
Cost	🔴	🔴	○	▦	🔴	▦	▦	▦
Scalability	🔴	🔴	▦	▦	🔴	▦	●	●
Ease of application	🔴	🔴	○	▦	🔴	▦	⊞	⊞
Engagement	●	●	○	●	●	●	🔴	🔴
Time commitment	🔴	▦	⊞	🔴	▦	▦	⊞	○

🔴 Very Good
▦ Good
○ Average
⊞ Poor
● Very Poor

The chart show pros and cons of various cyber security awareness methods

The MRO Subject Matter Expert Team is an industry stakeholder group which includes subject matter experts from MRO member organizations in various technical areas. Any materials, guidance, and views from stakeholder groups are meant to be helpful to industry participants; but should not be considered approved or endorsed by MRO staff or its board of directors unless specified.

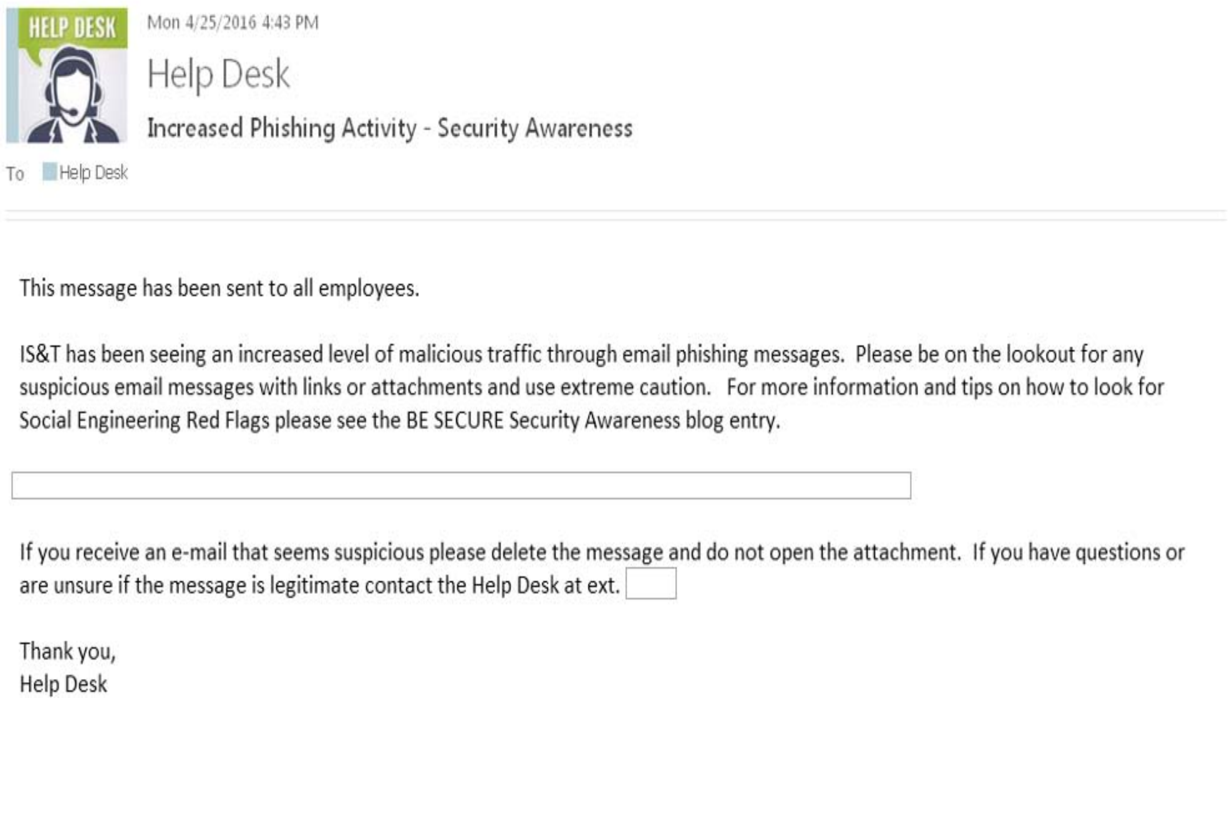
Direct Communication

E-mails

Application: Send to all personnel with access for quick dissemination of security threats.

Evidence: Copy of sent emails.

Example of email communication



Mon 4/25/2016 4:43 PM

Help Desk

Increased Phishing Activity - Security Awareness

To Help Desk

This message has been sent to all employees.

IS&T has been seeing an increased level of malicious traffic through email phishing messages. Please be on the lookout for any suspicious email messages with links or attachments and use extreme caution. For more information and tips on how to look for Social Engineering Red Flags please see the BE SECURE Security Awareness blog entry.

If you receive an e-mail that seems suspicious please delete the message and do not open the attachment. If you have questions or are unsure if the message is legitimate contact the Help Desk at ext.

Thank you,
Help Desk

The email contains the sent date

Memos

Application: Send to all new employees and contractors prior to issuing access. Many vendors offer monthly newsletters that entities may use as their memo.

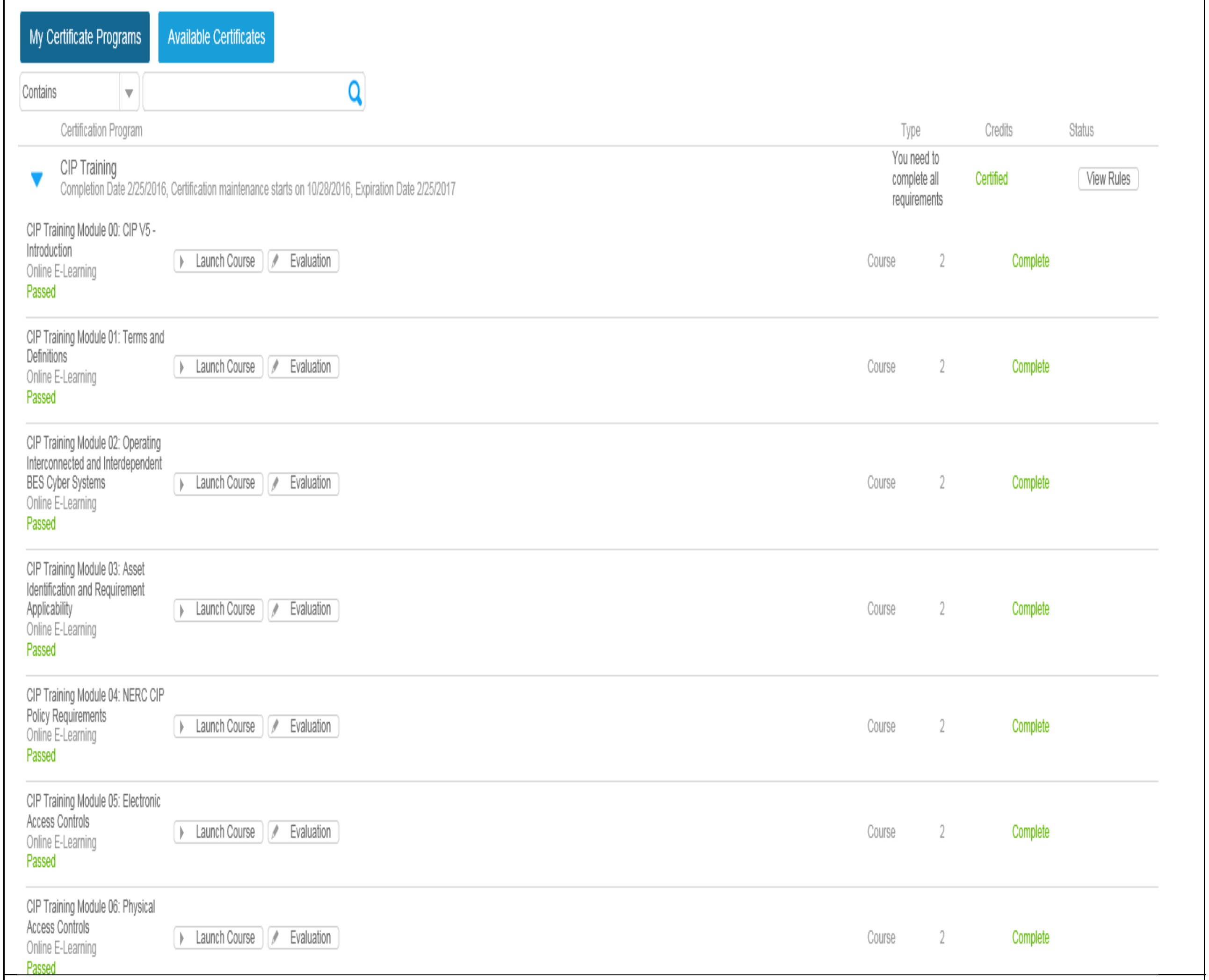
Evidence: Copy of dated memo.

Computer-based training

Application: Training used for High or Medium Impact BES Cyber Systems training requirements can also be used as evidence for low impact BES Cyber Systems requirements.

Evidence: Records of computer based training completion.

Example of computer based training



Certification Program		Type	Credits	Status
▼ CIP Training Completion Date 2/25/2016, Certification maintenance starts on 10/28/2016, Expiration Date 2/25/2017		You need to complete all requirements	Certified	View Rules
CIP Training Module 00: CIP V5 - Introduction Online E-Learning Passed	Launch Course · Evaluation	Course	2	Complete
CIP Training Module 01: Terms and Definitions Online E-Learning Passed	Launch Course · Evaluation	Course	2	Complete
CIP Training Module 02: Operating Interconnected and Interdependent BES Cyber Systems Online E-Learning Passed	Launch Course · Evaluation	Course	2	Complete
CIP Training Module 03: Asset Identification and Requirement Applicability Online E-Learning Passed	Launch Course · Evaluation	Course	2	Complete
CIP Training Module 04: NERC CIP Policy Requirements Online E-Learning Passed	Launch Course · Evaluation	Course	2	Complete
CIP Training Module 05: Electronic Access Controls Online E-Learning Passed	Launch Course · Evaluation	Course	2	Complete
CIP Training Module 06: Physical Access Controls Online E-Learning Passed	Launch Course · Evaluation	Course	2	Complete

The computer based training record contains date completed

Indirect Communications

Posters

Application: Place at physical entry points or high traffic areas at assets containing low impact BES Cyber Systems. Posters are often available from Cyber Asset vendors at little or no cost.

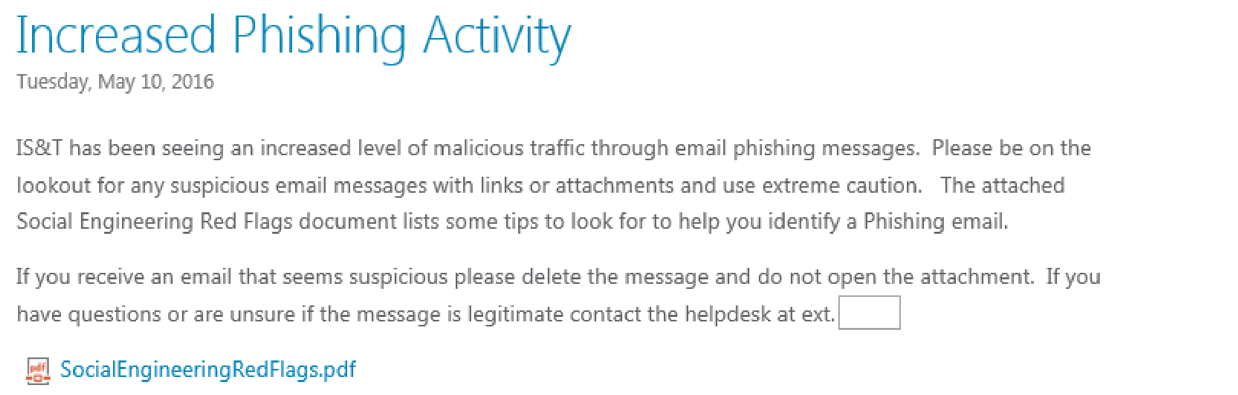
Evidence: Picture of hanging poster with dates posted.

Intranet

Application: Post articles reinforcing cyber security practices on the Intranet webpage that personnel with access to low impact BES Cyber Systems are likely to view.

Evidence: Screen shot of the intranet article with a date.

Example of an intranet article



Increased Phishing Activity

Tuesday, May 10, 2016

IS&T has been seeing an increased level of malicious traffic through email phishing messages. Please be on the lookout for any suspicious email messages with links or attachments and use extreme caution. The attached Social Engineering Red Flags document lists some tips to look for to help you identify a Phishing email.

If you receive an email that seems suspicious please delete the message and do not open the attachment. If you have questions or are unsure if the message is legitimate contact the helpdesk at ext. [redacted]

SocialEngineeringRedFlags.pdf

The article contains the posting date

Brochures

Application: Provide to new employees and contractors or at meetings

Evidence: Copy of brochure and distribution dates

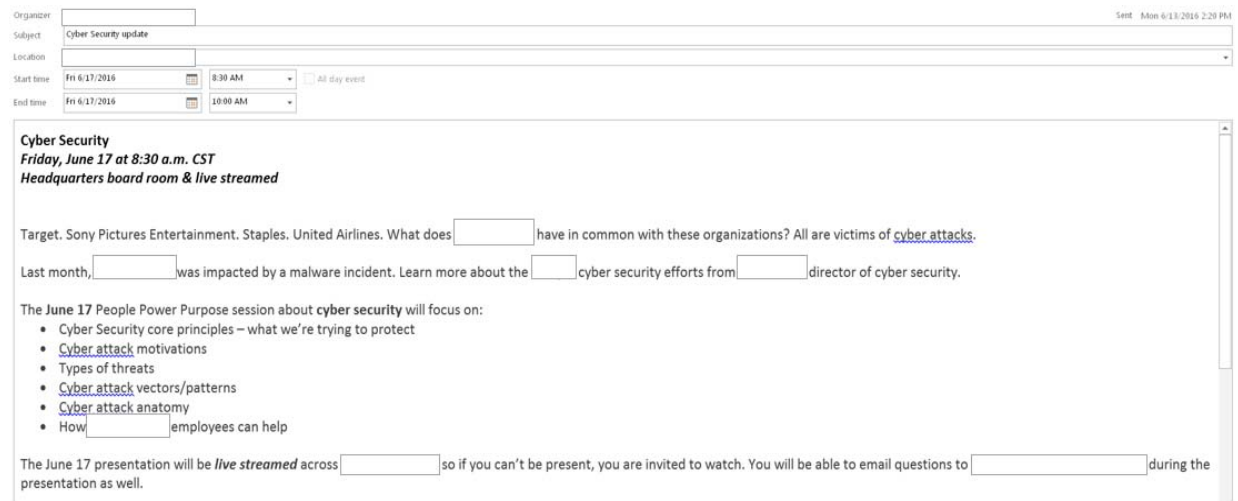
Management Support

Presentations

Application: Provide in-person awareness presentations about company policies and emerging threats to management and personnel with access to low impact BES Cyber Systems

Evidence: Dated slide deck and/or minutes for the meeting at which it was presented

Example of a presentation



Organizer [redacted]

Sent Mon 6/13/2016 2:20 PM

Subject Cyber Security update

Location [redacted]

Start time Fri 6/17/2016 8:30 AM □ All day event

End time Fri 6/17/2016 10:00 AM

Cyber Security
Friday, June 17 at 8:30 a.m. CST
Headquarters board room & live streamed

Target. Sony Pictures Entertainment. Staples. United Airlines. What does [redacted] have in common with these organizations? All are victims of cyber attacks.

Last month, [redacted] was impacted by a malware incident. Learn more about the [redacted] cyber security efforts from [redacted] director of cyber security.

The **June 17** People Power Purpose session about **cyber security** will focus on:

- Cyber Security core principles – what we're trying to protect
- Cyber attack motivations
- Types of threats
- Cyber attack vectors/patterns
- Cyber attack anatomy
- How [redacted] employees can help

The June 17 presentation will be ***live streamed*** across [redacted] so if you can't be present, you are invited to watch. You will be able to email questions to [redacted] during the presentation as well.

The slide deck from this presentation

Meetings

Application: Provide updates to management on status of cyber and physical security. While this means provides little for direct awareness, it indicates management support and can help allocate needed resources effectively

Evidence: Dated meeting minutes

Special Case Considerations

Outages

During planned or unplanned outages, entities commonly have many contractors and employees accessing locations physically and electronically. Along with the increase of access, there is often additional activity and other considerations for outages. For these reasons, entities may want to consider using passive means to provide cyber security awareness, tailoring current process to include awareness, or addressing awareness in contracts.

A good method to provide passive awareness is to install posters or signs at access points. This can be deployed both physically and electronically. Signs can be attached to gates, posters can be hung on doors, and desktop backgrounds can be set on computers.

Tailoring current processes to include awareness can also be effective. If employees and contractors must attend a kickoff meeting or safety briefing, handing out brochures and adding a short presentation about security awareness can meet compliance requirements.

Entities can incorporate contract language to address security awareness. This language could provide security awareness directly or obligate the contracted company to address security awareness items with applicable employees.

Teleworkers

Teleworkers miss out on physical forms of security awareness. To keep teleworkers aware, entities may consider using emails and Intranet articles.

Tours and Visitors

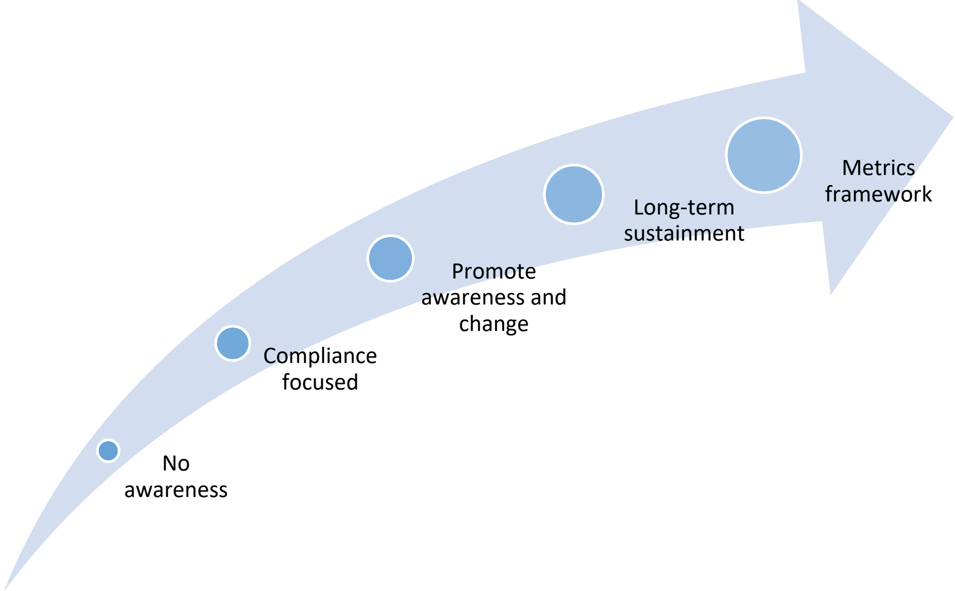
Entities often host tours and visitors, and thereby allow physical access to Low Impact BES Cyber Systems. For tours and visitors, an escort typically guides the group. The escort could make a brief security statement prior to entering the facility. Posters and signs at access points could also provide security awareness.

Beyond Compliance

While this document’s primary focus is guidance with applying compliance required security controls, security awareness should not be limited to the absolute minimum. Entities may find business benefits from maturing their security awareness program beyond a compliance focus.

Regardless, compliance requirements should be met prior to expanding the program. Programs often follow the progression shown below.

Security Awareness Progression



Entities may progress beyond compliance but should meet compliance requirements first

Entities often begin with no awareness programs. Reliability Standards can be the start of a security awareness program entities should:

a. Identify Reliability Standards
b. Coordinate with the internal compliance office
c. Develop or purchase methods to meet these requirements
d. Deploy security awareness

If the entity decides to progress beyond Reliability Standards, the entity will promote awareness and change. During this phase, entities:

a. Identify stakeholders
b. Identify the purpose and goals of the awareness program
c. Create a baseline of the current awareness level
d. Identify the target audiences, their specific needs, and program objectives
e. Determine what and how to communicate in an engaging program
f. Have the most senior stakeholder present the program
g. Execute the program and explain the purpose

After the program is promoted and implemented, begin long-term sustainment which includes:

a. Review program annually
b. Identify technological, threat, business, revised Reliability Standards
c. Assess your organization's awareness level and compare to the baseline
d. Collect feedback
e. Determine which methods have the greatest impact
f. Apply changes to program

In the final phase, entities may want to set up a metrics framework. This includes:

a. Identify key metrics to business outcomes
b. Execute metrics measurement
c. Communicate results on a schedule
d. Identify impact

Below are some potential metrics to consider tracking

- Number of victims of a phishing assessment
- Number of infected systems
- Number of reported incidents
- Number of people exposed to the awareness program
- Number of weak or shared passwords
- Percent of users with a positive attitude towards information security
- Percent of users who believe their actions impact security

Physical Security Controls (Attachment 1, Section 2)

Entities shall implement one or more documented cyber security plans addressing physical security controls. Entities are required to control physical access to assets or locations with low impact BES Cyber Systems and LEAP based on need as determined by the entity. Physical security controls manage physical access. These controls can be in a variety of types including:

- Operational & procedural controls: policies and rules
- Access controls: card key, locks, gates, barricades, etc.
- Monitoring controls: alarm systems, cameras, human observation, etc.
- Technical controls

The CIP Senior Manager should be able to justify the level of controls used. A variety of factors can be taken into consideration when deciding what controls to implement such as:

- Cost: initial price and reoccurring expenses
- Maintenance: required effort to keep the system functioning effectively
- Complexity: difficulty to control, manage, and operate
- Flexibility: capability for extension and repositioning
- Scalability: capability to expand for growth

For the best security, a defense in depth or layering of security controls should be implemented. A defense in depth strategy or costly controls may not be feasible or practical for every entity. Risk to the entity should be taken into consideration. Risk levels and risk tolerance will vary by entity and facility.

Physical Security Control Methods

NERC recognizes access controls; monitoring controls; operational, procedural, and technical controls as physical security controls. These should be implemented as defined in the entities security plan. Each type of control has benefits and detriments. Detriments can often be offset by layering the controls. The entity is responsible for deciding which control(s) best meet their requirements and the CIP Senior Manager should be able to justify the security decisions.

Access Controls and Monitoring Controls

Access controls regulate who or what can enter an environment. Many access controls exist, including:

- Fences with locked gates
- Locked doors
- Locked cabinets
- Barricades
- Proxy card locks
- Cipher locks

Monitoring controls identify and alert when someone or something enters an environment. Many monitoring controls exist, including:

- Door alarms
- Motion detectors
- Cameras
- Human observation
- Pressure plate alarms
- Card access alarms

Operational, Procedural, and Technical Controls

Operational and procedural controls mitigate risks through policies, procedures or guidelines. They rely on user to follow rules and guidelines to be effective. A few examples include procedures, guidelines, and polices regarding:

- Check-in and checkout
- Reporting procedures
- Employee monitoring
- Vulnerability assessments
- Separation of duties
- Access removal
- Contingency planning
- Identification and authentication
- Training
- System maintenance
- Media protection
- Personnel sanctions
- Risk assessment
- Acquisition policy
- Operation security
- Compartmentalization

Technical controls use technology as a basis for controlling the access and usage of sensitive data throughout a physical structure and over a network.

Physical Access and Monitoring Controls

Table of Pros and Cons of Physical Access and Monitoring Controls

	Locked gates & fence	Locked doors & cabinets	Card access control	Cipher locks	Door alarms	Cameras & lighting	Posted guard
Cost	🔴	🔴	○	◍	◍	⊞	⚫
Maintenance	◍	◍	🔴	🔴	○	⊞	⚫
Complexity	🔴	🔴	○	◍	○	⊞	🔴
Flexibility	⊞	⊞	◍	◍	◍	🔴	🔴
Scalability	⊞	⊞	🔴	🔴	⊞	○	⚫

🔴 Very Good
◍ Good
○ Average
⊞ Poor
⚫ Very Poor

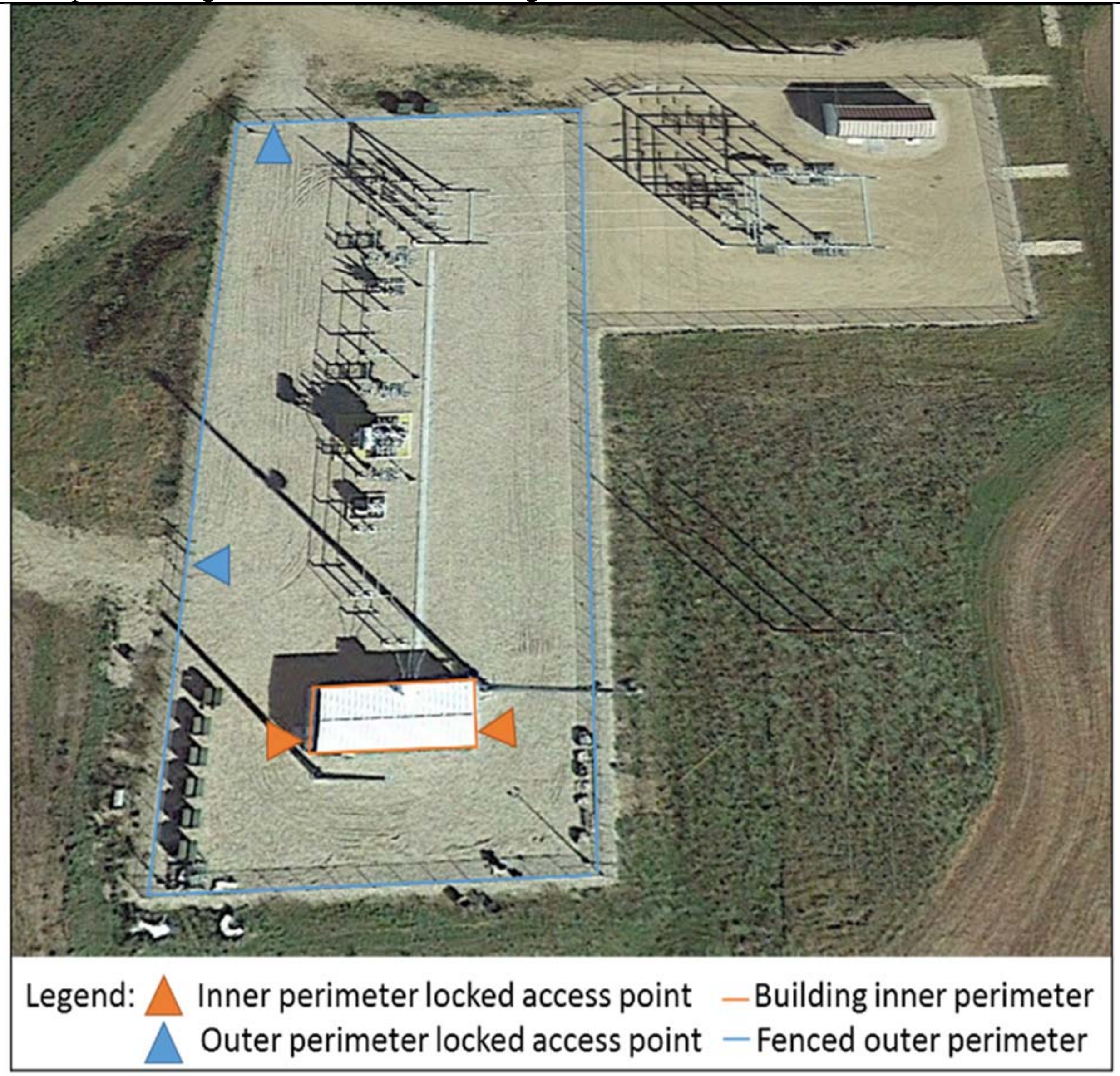
The table show pros and cons of access and monitoring controls

The MRO Subject Matter Expert Team is an industry stakeholder group which includes subject matter experts from MRO member organizations in various technical areas. Any materials, guidance, and views from stakeholder groups are meant to be helpful to industry participants; but should not be considered approved or endorsed by MRO staff or its board of directors unless specified.

Fences with Locked Gates

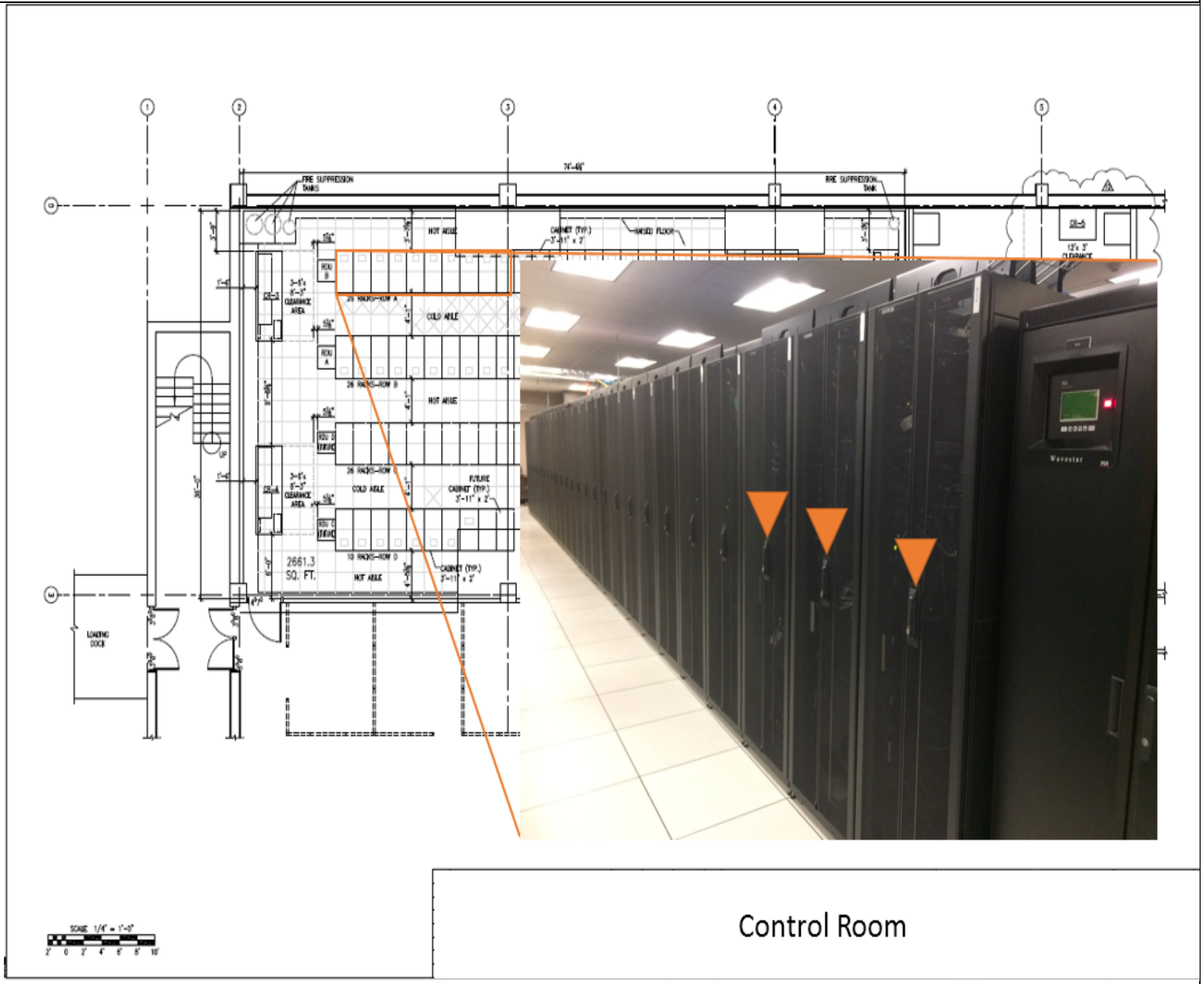
Application: Fences are likely already in place and can encompass the perimeter of the BES asset. Fences and locked gates can be easily layered with other access control. Managing keys can be difficult. Gates can be remote controlled and/or motorized. Controlling access with these types of gates increases cost and complexity greatly but mitigates maintenance issues with key management.

Evidence: Copies of drawings, photographs, or diagrams identifying fences and locked gates or physical inspections of the assets containing Low Impact BES Cyber Systems and LEAPs.

Example of a diagram of fences with locked gates
 Legend: ▲ Inner perimeter locked access point — Building inner perimeter ▲ Outer perimeter locked access point — Fenced outer perimeter
Locations of the fence and locked access point are identified

Locked Doors and Cabinets

Application: Doors likely already have locks in place, but managing keys can be difficult. Locking cabinet would be applied in the same manner as doors but offer the ability to limit the area entities are responsible to control access. Limiting the area of responsibility can greatly reduce workload and focus security resources.
Evidence: Copies of drawings, photographs, or diagrams identifying locked doors and cabinets or physical inspections of the assets containing low impact BES Cyber Systems and LEAPs.

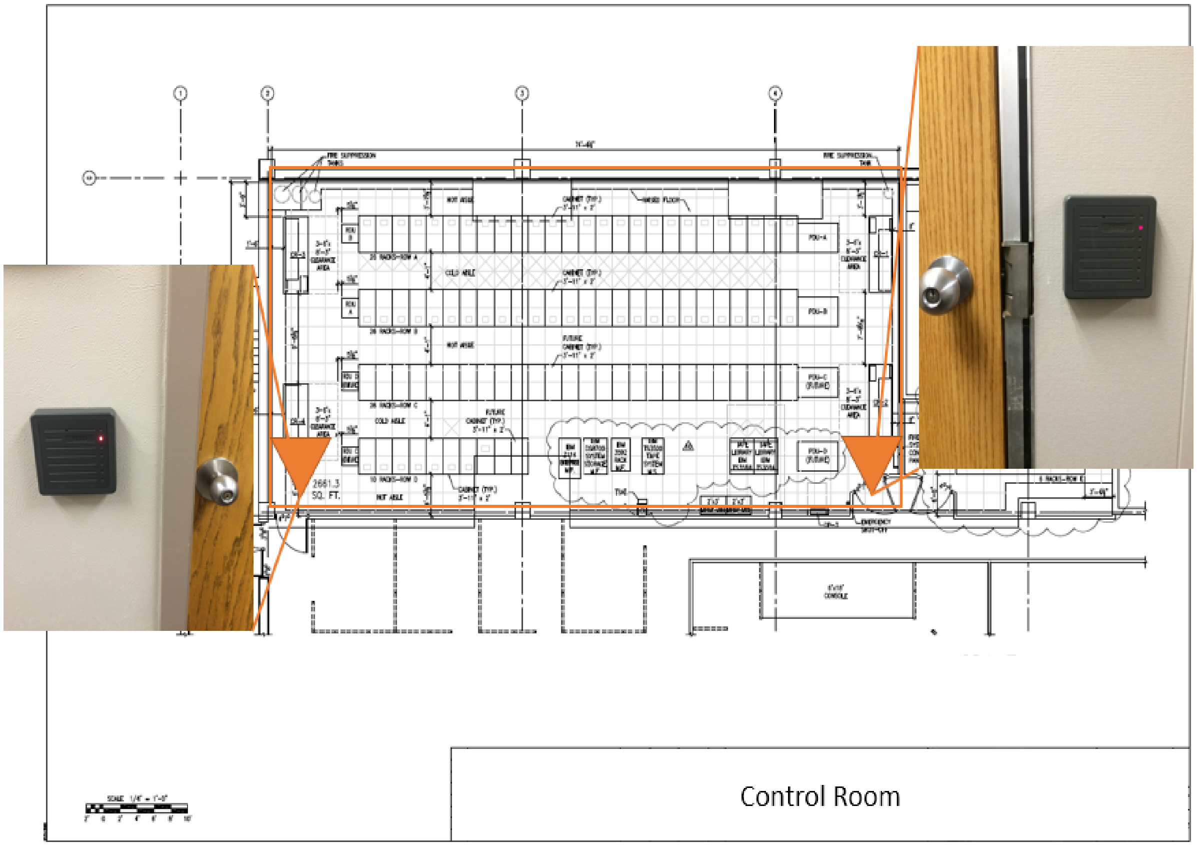
Photographs of locked cabinets
 HOT AISLE COLD AISLE 2661.3 SQ. FT. LOADING DOCK SCALE 1/4" = 1'-0" Control Room
These photographs identify the control used and are labeled to show the areas protected

Proxy Card Control

Application: Installing proxy card control locks reduces the difficulty of managing keys and is very easy to remove/grant access and audit.

Evidence: Copies of drawings, photographs, or diagrams identifying proxy card controlled access points; physical inspections of the assets containing low impact BES Cyber Systems and LEAPs; or documentation of access lists.

Drawing and photographs of proxy card controls



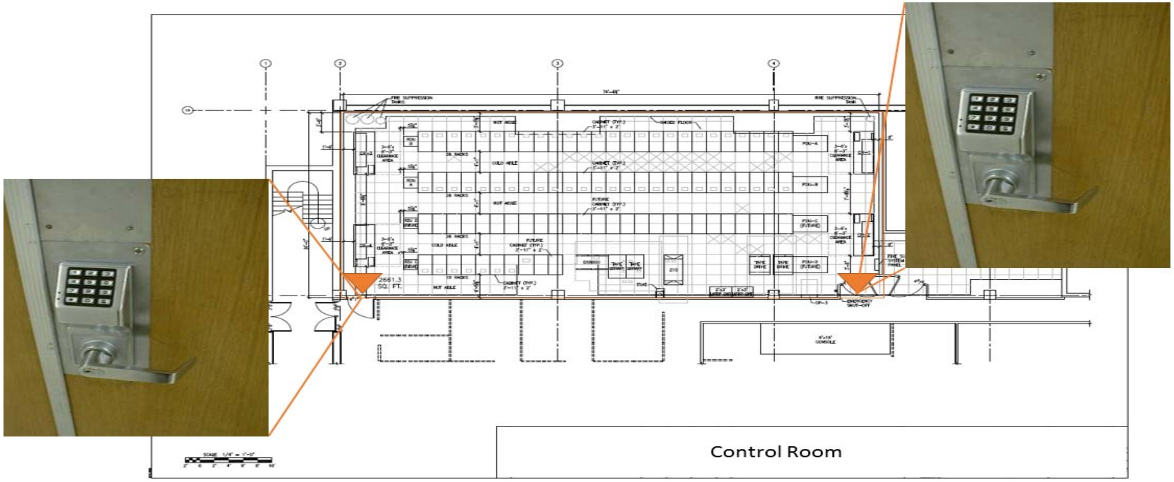
These photographs identify the control used and are labeled to show the areas protected

Cipher Lock Control

Application: Installing cipher locks reduces the difficulty of managing keys, and it is less expensive to change codes than to rekey locks.

Evidence: Copies of drawings, photographs, or diagrams identifying proxy card controlled access points; physical inspections of the assets containing low impact BES Cyber Systems and LEAPs; or documentation of access code distribution.

The MRO Subject Matter Expert Team is an industry stakeholder group which includes subject matter experts from MRO member organizations in various technical areas. Any materials, guidance, and views from stakeholder groups are meant to be helpful to industry participants; but should not be considered approved or endorsed by MRO staff or its board of directors unless specified.

Photographs of cipher lock controls

These photographs identify the control used and are labeled to show the areas protected

Door Alarms

Application: Installing door alarms on doors that protect low impact BES Cyber Systems and LEAPs.

Evidence: Copies of drawings, photographs, or diagrams identifying the door alarms; physical inspections of the assets containing low impact BES Cyber Systems and LEAPs.

Cameras and Lighting

Application: Installing camera systems that monitor access point and/or the perimeter for BES Cyber Systems and LEAPs. Lighting combined with procedural controls for monitoring can provide monitoring control.

Evidence: Copies of drawings, photographs, or diagrams identifying the cameras; physical inspections of the assets containing low impact BES Cyber Systems and LEAPs.

Posted Guard

Application: Hiring a posted guard(s) to control physical access. This will often not be practical for many entities but provides good security and flexibility.

Evidence: Documentation of guard information and security roles regarding low impact BES Cyber Systems and LEAPs, physical inspections of the assets containing low impact BES Cyber Systems and LEAPs.

Special Case Considerations

- Outages

  During outages, the number of personnel accessing low impact BES Cyber Systems may increase significantly. It is important to ensure the selected security controls can accommodate a large influx of workers for those events.

- Tours and Visitors

During tours and with visitors, it is advisable to implement procedural controls. Having a visitor escort procedure can cost effectively meet requirements.

- Geographically Separated Locations

  Entities with larger sites often have facilities and assets that are geographically separated from the primary site. In these situations, where the geographically separated location contains BES Cyber Systems or a LEAP, the geographically separated location still requires one or more security control(s) and documentation in the plan for BES Cyber Systems protected by the controls. The CIP Senior Manager should be able to justify if the security control is appropriate for the situation. A locked door or cabinet securing the low impact BES Cyber Systems or LEAP in the geographically separated location can often be a good solution.

Beyond Compliance

The equations below can help entities determine if security measures are cost effective but are NOT required for compliance.

Single Loss Expectancy Formula
$AV * EF = SLE$ Asset Value (AV): worth of a resource to the organization Exposure Factor (EF): percent of the asset lost from a successful threat Single Loss Expectancy (SLE): loss expected for any single successful threat
Calculates loss expected for any single successful threat

Annual Loss Expectancy Formula
Single Loss Expectancy (SLE): monetary cost expected from the occurrence of a risk Annual Rate of Occurrence (ARO): probability that a risk will occur in a year Annual Loss Expectancy (ALE): loss expected due to a risk over a year $SLE * ARO = ALE$
Calculates loss expected for year from a threat

Cost Effectiveness Formula
Security Measure (SM): Annual cost of a security measure Annual Loss Expectancy (ALE): loss expected due to a risk over a year If $SM > ALE$, then security measure is NOT cost effective If $SM < ALE$, then security measure is cost effective
Determines cost effectiveness of security measures

Examples
Asset Value (AV): A loss of a 600MW coal plant for 24 hours is $1,000,000 Exposure Factor (EF): Remote-controlled malware triggered a plant shutdown, requiring 6 hours for root cause analysis and quarantine, and 12 hours for plant cold-start recovery. No damage to plant occurred during shutdown. (6 hours +12 hour)/24 hours = 75%

Single Loss Expectancy (SLE): AV * EF = SLE = $1,000,000 * 75% = $750,000 Annual Rate of Occurrence (ARO): once in 25 years 1/25=0.04 SM1: Annual cost of manning a 24/7 manned Cyber Operations Center is $150,000 SM2: Annual amortized capital, administrative and software maintenance costs for an Intrusion Detection System and Incident Response team = $5,000 AV x EF = SLE ; $1,000,000 * 75% = $750,000 SLE x ARO = ALE ; $750,000 * 0.04 = $30,000 SM1 > ALE ; $150,000 > $30,000 It would NOT be cost effective to implement a 24/7 manned Cyber Operations Center for this single loss scenario. SM2 < ALE ; $5,000 < $30,000 It would be cost effective to implement an Intrusion Detection System and Incident Response team.
Provides an example of cost effectiveness for two security measures

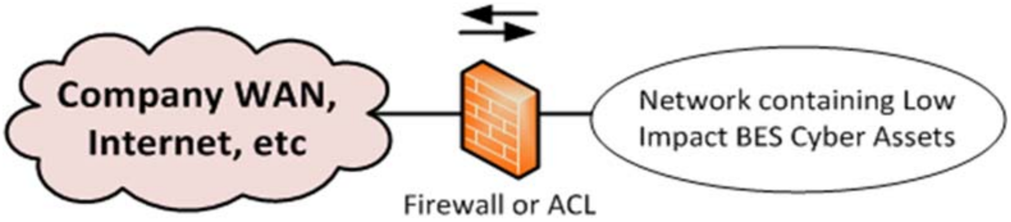
Electronic Access Controls (Attachment 1, Section 3)

CIP-003-6 R1.2.3 requires that all sites containing low impact BES Cyber Systems implement "electronic access controls for LERC and Dial-up Connectivity". CIP-003-6 Attachment 1 further specifies the following:

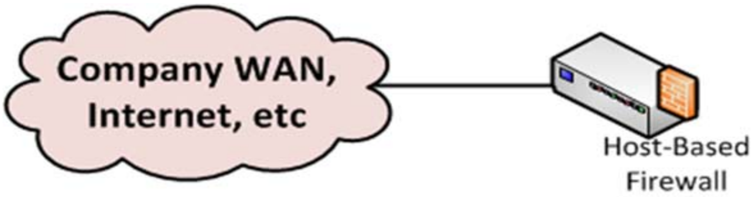
- For LERC, implement a LEAP to permit only necessary inbound and outbound bi-directional routable protocol access.
- Implement authentication for all Dial-up connectivity, if any, that provide access to low impact BES Cyber Systems, per Cyber Asset capability.

In the LERC case, the LEAP is essentially the gatekeeper between the "outside world" and the protected Low Impact BES Cyber System. For Low Impact BES Cyber Systems there is no explicit ESP defined, but it is required to define an access point that provides control. The analogous system in medium and high Impact BES Cyber Systems scenarios is the Electronic Access Point (EAP) that protects the ESP.

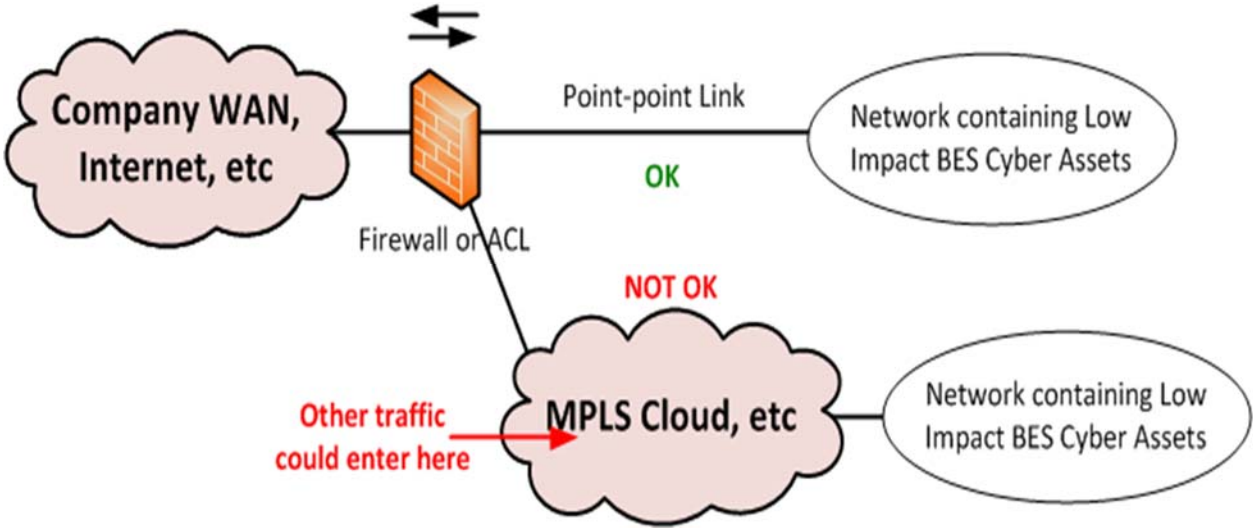
The LERC requirement is most easily understood by considering a standard network firewall or router access control list (ACL). These devices inspect Internet Protocol (IP) packets, looking at information such as source and/or destination IP address, source/destination port, etc. The "only necessary" part of the requirement points to needing a ruleset with a "deny all" rule, causing any traffic not explicitly allowed in other rules to be denied/dropped.


Company WAN, Internet, etc
Firewall or ACL
Network containing Low Impact BES Cyber Assets

Note that LEAPs can be internal to the BES asset or a BCA, e.g. a host-based firewall installed on the device.



Finally, it is permissible for the LEAP to reside at a remote location from the BES assets containing low impact BES Cyber Systems protected as long as all communication to those low impact BES Cyber Systems passes through the LEAP. The location of the remote LEAP would need physical protection per Attachment 1 Section 2.


Company WAN, Internet, etc
Point-point Link
Network containing Low Impact BES Cyber Assets
OK
Firewall or ACL
NOT OK
Other traffic could enter here
MPLS Cloud, etc
Network containing Low Impact BES Cyber Assets

Special Consideration: Vendor Access

As electronic systems become more and more complex, it is typical for equipment vendors to request a remote access path for assistance in troubleshooting. This is potentially a dangerous proposition as opening a BES Cyber System to a vendor exposes that system to any vulnerability in the vendor's systems.

For example, a vendor might request that an Internet-facing firewall be installed to allow them to VPN into the cyber system for remote support purposes. This not only makes the firewall vulnerable to attack from the Internet, but even if it is secure in that aspect it may provide a path for an attacker to gain access to the vendor network (which may be less secure) and then pivot to the Cyber System through the VPN.

Put simply, extreme caution and extra protective measures should be taken regarding vendor access to BES Cyber Systems.

LERC (Routable Connectivity) Example (Attachment 1, Section 3.1)

The standard requirement is not prescriptive of how to implement "permit only necessary inbound and outbound" access. Using an inbound example, a rule could be written to allow Telnet access into the local network from anywhere:

Action	Source IP	Destination IP	Source Port	Destination Port	Notes
ALLOW	any	any	any	23/TCP	Telnet

This rule would not meet the language of the standard, given that unrestricted access would be allowed to the destination port. At a minimum, the source should be limited to a known IP range.

Action	Source IP	Destination IP	Source Port	Destination Port	Notes
ALLOW	[company network range]	any	any	23/TCP	Telnet

This would now at least require an attacker to be on the company network to communicate with low impact BES Cyber Systems. Even better would be to identify the individual users or systems that need access. *It is best practice to make rules as specific as possible.*

Action	Source IP	Destination IP	Source Port	Destination Port	Notes
ALLOW	[specific user IPs]	[local network range]	any	23/TCP	Telnet

Further note that the standard specifically states that outbound access must also be controlled. It is not permissible to allow local devices to communicate outbound unimpeded. It may seem that if the intent is to keep attackers out then only inbound rules are necessary, but if a system is compromised one of the things it is likely to do is "phone home" to the attacker's command and control system to potentially request further malware. Blocking this can limit the scope of the breach. Therefore, the following example of an outbound rule may not be implemented.

Action	Source IP	Destination IP	Source Port	Destination Port	Notes
ALLOW	[local network range]	any	any	any	Allow all outbound

Finally, to achieve the "permit only necessary..." access requirement, the LEAP must implement a "cleanup" or "deny all" rule. Firewalls evaluate network traffic against each rule in their ruleset for a match, and if found pass the traffic. They must therefore have a rule that does not pass traffic at the end of the ruleset. Traffic that does not match any of the specific rules moves down the list until it reaches the bottom, which is configured to match anything, and is blocked.

Action	Source IP	Destination IP	Source Port	Destination Port	Notes
DENY	any	any	any	any	cleanup

Therefore, the final ruleset will be a list of "necessary" communications (both inbound and outbound) and then a cleanup rule at the end. For example:

Action	Source IP	Destination IP	Source Port	Destination Port	Notes
ALLOW	[specific user IPs]	any	any	23/TCP	Telnet from engineering PCs
ALLOW	[local network range]	any	any	20000/TCP	DNP polls from local network to outside devices
DENY	any	any	any	any	Cleanup rule

Ideally the ruleset would be even more specific; as specific as absolutely possible.

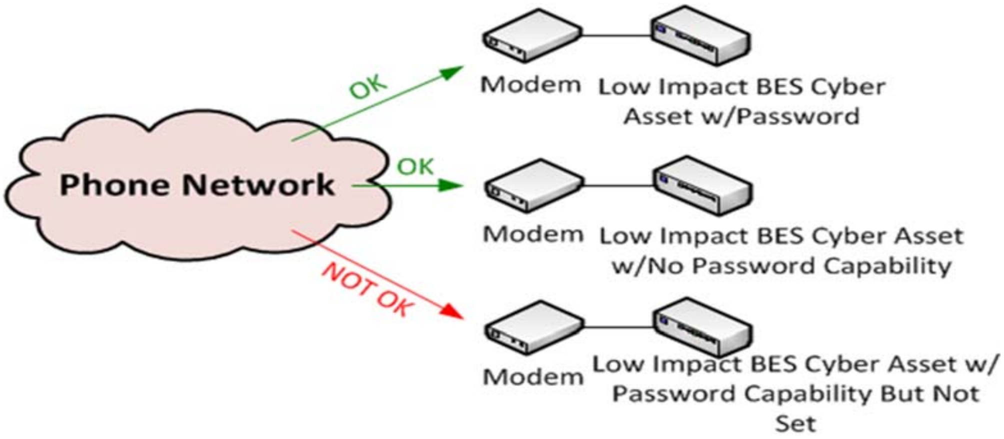
Action	Source IP	Destination IP	Source Port	Destination Port	Notes
ALLOW	[specific user IPs]	[specific devices]	any	23/TCP	Telnet from engineering PCs to telnet devices
ALLOW	[DNP master on local network]	[specific DNP client devices]	any	20000/TCP	DNP polls from master on local network to remote devices
DENY	any	any	any	any	Cleanup rule

*A "notes" field can be useful to provide documented justification for rules.

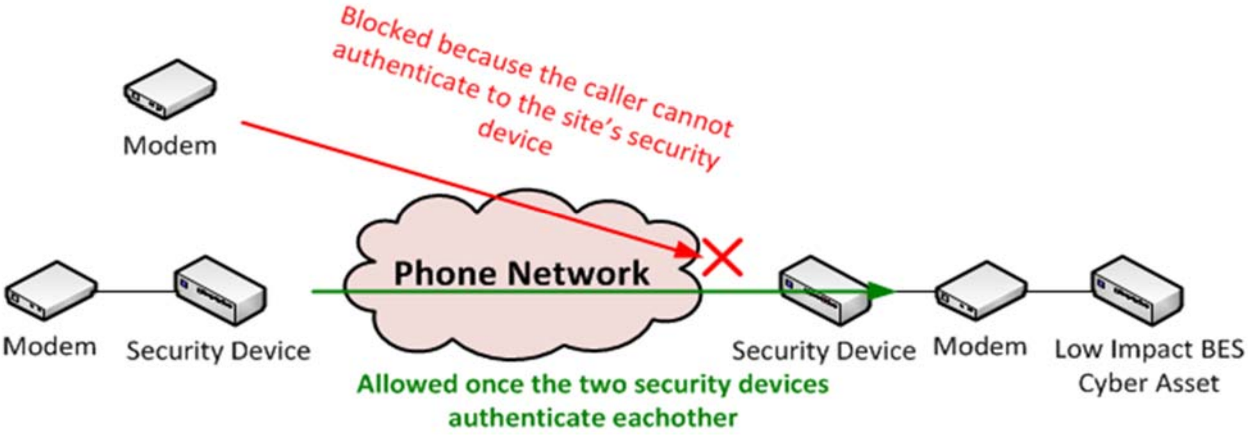
Dial-up Connectivity (Attachment 1, Section 3.2)

The dial-up connectivity requirement states that "authentication" must be in place for dial-up accessible devices "per Cyber Asset capability". Unlike the routable (LERC) requirement, this requirement can be met at either the overall location level (like the LEAP case), on the dial-up device, or on the individual BCA.

Looking at the latter case first, an example would be for a protective relay. Many protective relays provide the ability to set a login password. This would be sufficient to meet the requirement. Furthermore, due to the "per Cyber Asset capability" language, devices that do not have the capability for authentication may still be connected. In that case, it is strongly recommended to have an attestation from the vendor that passwords are not possible, or specific language from a device manual stating the same.


Phone Network
OK
Modem
Low Impact BES Cyber Asset w/Password
OK
Modem
Low Impact BES Cyber Asset w/No Password Capability
NOT OK
Modem
Low Impact BES Cyber Asset w/ Password Capability But Not Set

It is also possible to meet this requirement at the BES asset level as a whole, much like the LEAP in the LERC scenario. Dial-up "security gateway" devices are available that function to authenticate incoming communications. Most often they involve a paired device that the caller has connected to their modem which authenticates to the remote location device.


Blocked because the caller cannot authenticate to the site's security device
Modem
Phone Network
Modem
Security Device
Security Device
Modem
Low Impact BES Cyber Asset
Allowed once the two security devices authenticate eachother

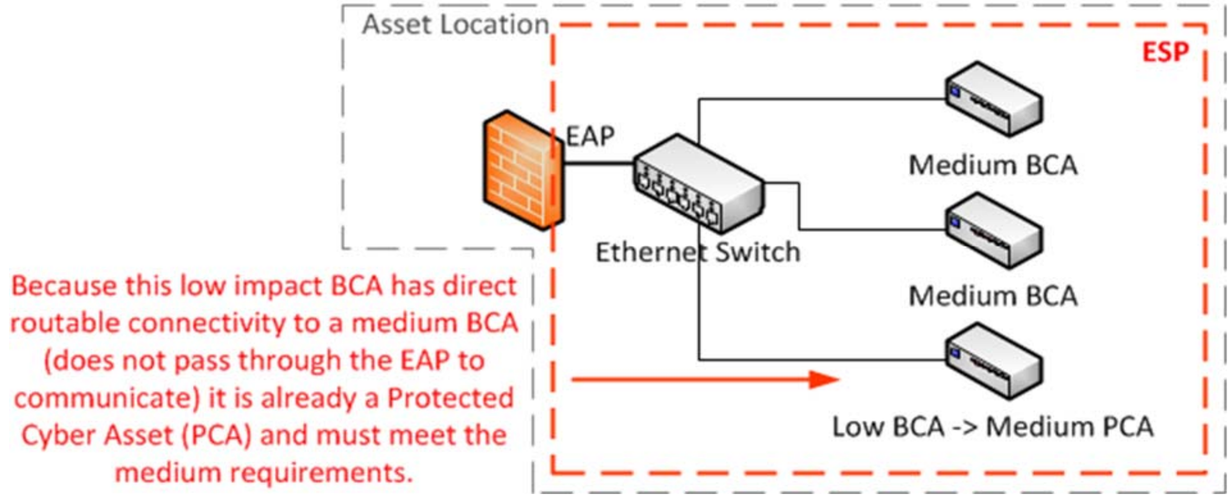
Sites with Low Impact and Medium/High Impact Cyber Systems

Sites with assets at multiple impact levels have two options:

- If grouped together, "high watermark" any lower impact level devices to those of the greatest present. This means they must be treated as if they are at the highest level and all applicable requirements apply.
- Segregate devices by classification and implement appropriate protection specific to each.

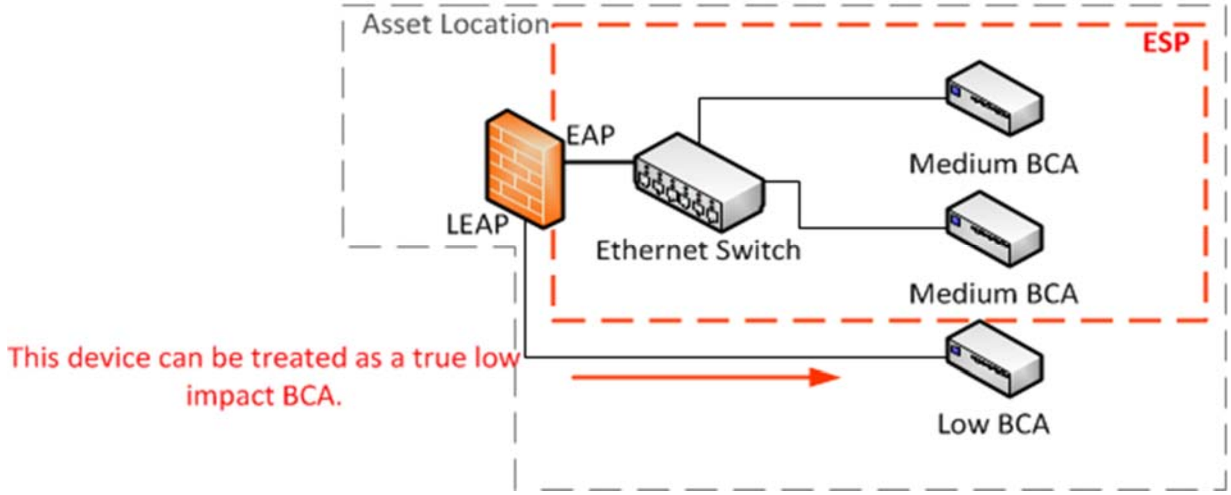
High Watermarking vs Segregating Low Impact Devices

If a low impact BES Cyber Systems shares a network with higher level devices and can communicate with them without passing through an EAP, then that low impact BES Cyber Systems is within the ESP and will be a Protected Cyber Asset (PCA) at the highest level of cyber system on that network. In this case, rather than meeting the low impact BES Cyber Systems, requirements the device would need to meet PCA requirements for the higher level.



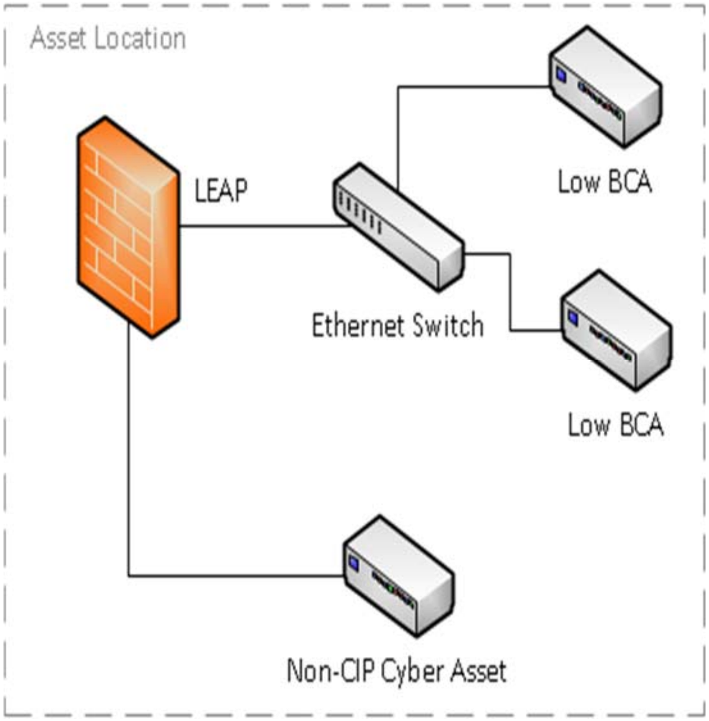
Because this low impact BCA has direct routable connectivity to a medium BCA (does not pass through the EAP to communicate) it is already a Protected Cyber Asset (PCA) and must meet the medium requirements.

Alternatively, the same network containing low impact BES Cyber Systems can be connected to a separate port on a security device (LEAP) if the device enforces security protections between the two ports. This limits the requirements put upon them, but now personnel must be aware of the different requirements and what cyber assets they apply to within the single physical BES asset. Also note that because the device providing the LEAP is also a Medium Impact EAP it must meet all the medium impact (Electronic Access Control or Monitoring Systems (EACMS) requirements.



This device can be treated as a true low impact BCA.

It should be noted that a device functioning as a LEAP may also have non-CIP devices connected to it, provided proper security controls are enforced for the traffic/access.



High Watermarking

Pros:

- Existing protections for medium or high impact BES Cyber Systems can be re-used
- Consistent designs and security procedures
- Consistent work practices for field personnel
- No need to add additional devices
- Increased security for low impact BES Cyber Systems

Cons:

- Increased controls for low impact BES Cyber Systems devices. If high watermarked they must meet all the technical and documentation requirements placed on the higher impact rating. For example, the requirements on low impact BES Cyber Systems do not specify the need for change control, patch management, malware monitoring, logging & alerting, etc. If low impact BES Cyber Systems devices are high watermarked these requirements likely come into play.

Segregating Low Impact BES Cyber Systems from High or Medium BES Cyber Systems

Pros:

- Avoids the increased requirements placed on high and medium impact BES Cyber Systems
- Provides a clear delineation between low and high or medium impact BES Cyber Systems

Cons:

- Personnel must keep track of different designs and processes for low and high or medium impact BES Cyber Systems
- Complicates design
- Likely adds additional hardware

Cyber Security Incident Response (Attachment 1, Section 4)

Responsible entities shall have one or more Cyber Security Incident response plan(s). The plan(s) shall cover:

- Identification, classification and response to Cyber Security Incidents
- Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing an Analysis Center (E-ISAC), unless prohibited by law
- Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals
- Incident handling for Cyber Security Incidents
- Testing the Cyber Security Incident response plan(s) at least every 36 calendar months by
    - Responding to an actual incident
    - Using a drill or tabletop exercise of a Reportable Cyber Security Incident
    - Using an operational exercise of a Reportable Cyber Security Incident
- Updating the Cyber Security Incident plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan test or actual Reportable Cyber Security Incident

The requirements are set, but entities have freedom for implementation. Plans can vary greatly. They can be detailed or simplistic; call for the use of outside entities or be internally managed; be rigid or flexible. The plan can also be applied via multiple methods such as:

- Using the entity's existing cyber security incident response plan
    - Using cyber security incident response plans for high and medium impact BES Cyber Systems
- Creating a stand-alone plan covering all BES assets containing low impact BES Cyber Systems
- Creating individual plan per type of BES asset, individual BES asset, or grouping of BES assets

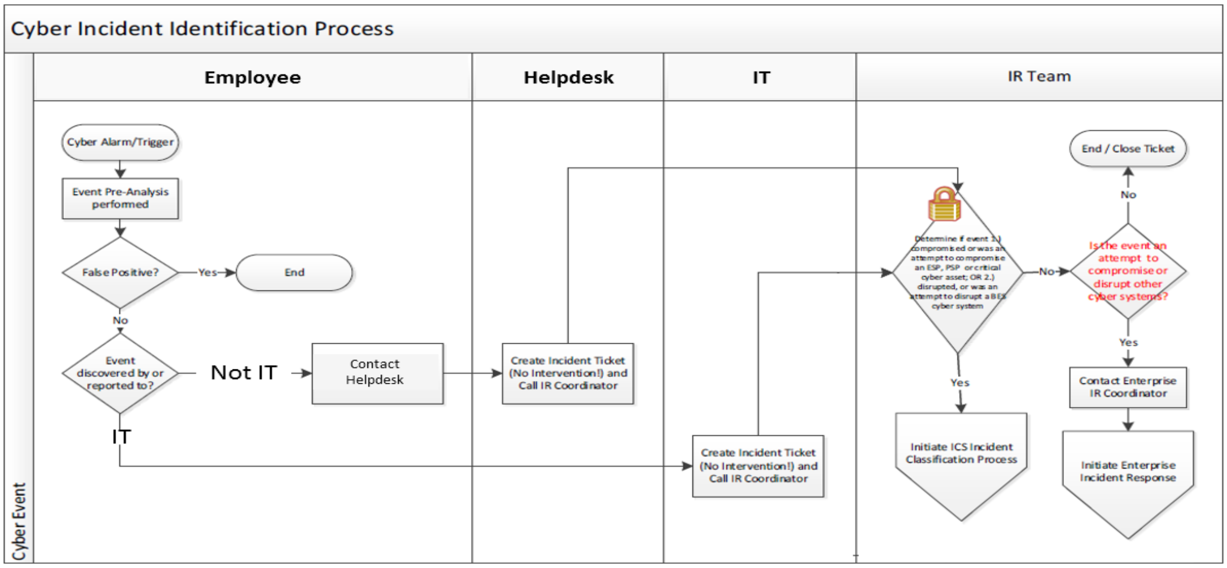
Regardless of how the plan is implemented, the CIP Senior Manager should be able to explain and justify the entities rationale for the level of Cyber Security Incident response plan. When developing an incident response plan, entities may want consider the following factors:

- Effectiveness: The most important factor for the plan is effectiveness, whether it works and how well. Different plans will work best for different entities
- Adaptability: The ability to allow the plan to change or have the flexibility to work for a variety of potential incidents
- Resource Requirements: The total resources needed to make the plan function (training, preparation, upkeep, outside resources, opportunity costs, etc.)
- Scalability: The ability to use this plan to cover multiple locations with few or no changes

Identification, Classification, and Response to Cyber Security Incidents (Attachment 1, Section 4.1)

Application: Document a process for identifying, classifying and responding to Cyber Security Incidents

Example Process for Identification


Cyber Incident Identification Process
Employee
Helpdesk
IT
IR Team
Cyber Event
Cyber Alarm/Trigger
Event Pre-Analysis performed
False Positive?
Yes
End
No
Event discovered by or reported to?
Not IT
IT
Contact Helpdesk
Create Incident Ticket (No Intervention!) and Call IR Coordinator
Create Incident Ticket (No Intervention!) and Call IR Coordinator
Determine if event 1.) compromised or was an attempt to compromise an ESP, PSP or critical cyber asset; OR 2.) disrupted, or was an attempt to disrupt a BES cyber system
Yes
Initiate ICS Incident Classification Process
No
Is the event an attempt to compromise or disrupt other cyber systems?
No
End / Close Ticket
Yes
Contact Enterprise IR Coordinator
Initiate Enterprise Incident Response

Flowchart is documented in the Incident Response Plan

Evidence: Documented process in the Incident Response Plan

Examples of Triggers

Trigger – Events

A security event is a potential indication that the security of information, information systems, services, or networks may have been breached or compromised. Indications of potential security events include, but are not limited to:

- Slow system response time
- Inability to access system resources
- Unexplained new files or unfamiliar file names
- Unexplained modifications to file lengths and/or dates
- Unexplained modification or deletion of data
- Unexplained new user accounts
- Unsuccessful log-on attempts
- Downed system with suspicious circumstances related to the outage
- Unusual messages (errors, pop-ups, etc.)

Trigger – Incidents

A security incident is any adverse activity that compromises the confidentiality, integrity, or availability of [ENTITY NAME's] information resources, or results in non-compliance with [ENTITY NAME] Security Policies and Procedures. Examples of security incidents include, but are not limited to:

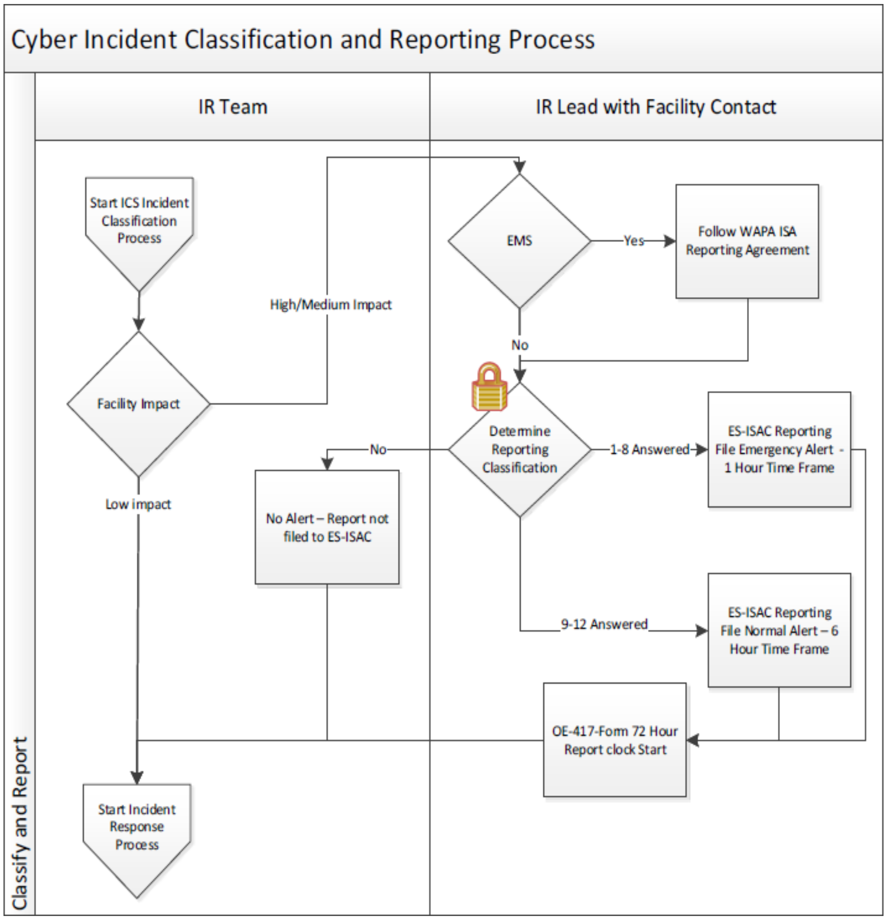
- Malware Infection – The presence of software designed specifically to disrupt a computer system (e.g., viruses, Trojan horse, worm, ransomware, spyware)
- Fraudulently acquiring sensitive information such as user IDs, passwords, and

financial account information

- Denial of Service (DoS) – An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources
- Damaged or unauthorized modification to data
- Unauthorized Access – Gaining unauthorized electronic access to information or to a network, system, application, or data
- Theft or loss of [ENTITY NAME] computer equipment or data (e.g., laptop, DVD, thumb drive, personal devices that house [ENTITY NAME's] data)

Triggers are documented in the Incident Response Plan

Example Process for Classification and Reporting


Cyber Incident Classification and Reporting Process
Classify and Report
IR Team
IR Lead with Facility Contact
Start ICS Incident Classification Process
Facility Impact
High/Medium Impact
Low impact
EMS
Yes
Follow WAPA ISA Reporting Agreement
No
Determine Reporting Classification
1-8 Answered
ES-ISAC Reporting File Emergency Alert - 1 Hour Time Frame
No
No Alert – Report not filed to ES-ISAC
9-12 Answered
ES-ISAC Reporting File Normal Alert – 6 Hour Time Frame
OE-417-Form 72 Hour Report clock Start
Start Incident Response Process

Flowchart is documented in the Cyber Security Incident response plan

Report Determination (Attachment 1, Section 4.2)

Application: A good option is to follow OE 417 reporting criteria

Evidence: Identify that OE 417 will be followed in the Incident Response Plan

Example of Reporting Procedures
The incident plan should make reference to the following: NERC Critical Infrastructure Protection (CIP) Standards require identification of reportable cyber security incidents. [ENTITY NAME] has defined reportable cyber security incidents as those identified on the Department of Energy's (DOE) Form OE-417, Electric Emergency Incident and Disturbance Report. **Filing Criteria:** • Within 1 Hour of Incident: A cyber event that causes interruptions of electrical system operations. • Within 6 Hours of Incident: A cyber event that could potentially impact electric power system adequacy or reliability. For reportable events go to https://www.oe.netl.doe.gov/oe417.aspx and take the following actions: 1. Under OE-417 Online Submissions, click on the Online OE-417 Survey Form, click OK, and then click on Submit without registering an account. 2. Fill out Section I. 3. Click on the Recipients tab and within Notify NERC, click on Yes. 4. Click Review and if everything is correct, click Submit. **Phone Contacts:** DOE: 202-586-8100 E-ISAC: 404-446-9780 (#2)
Reporting procedures are documented in the Cyber Security Incident response plan

Roles and Responsibilities (Attachment 1, Section 4.3)

Identifying roles and responsibilities is essential for an Incident Response Plan to work. Personnel need to know what they are responsible to do and how they interact with others. It is also helpful for distributing workload and fixing deficiencies in a plan.

Application: The organizational structure can be different for each entity. In order for an Incident Response Plan to be effective, the roles and responsibilities of applicable personnel needs to be identified and understood. This can be identified in:

- Processes
- Procedures
- Separate document(s)

Evidence: Copy of document(s) used to identify roles and responsibilities.

Example of Identified Roles and Responsibilities
Users • All users should report cyber security events and incidents to the [ENTITY NAME]

Help Desk with the exception of information security procedure violations. Procedure violations should be reported to your supervisor/manager (e.g., inappropriate use of email or Internet, unauthorized access to information).

- All physical security events or incidents should be reported to Facilities Management.

Supervisors/Managers

- Report information security procedure violations to the Director - Information Security or the Manager – Security Compliance

Director In-Charge

The Director - Information Security is assigned this role.

- Communicate security incident information to the Chief Information Officer or equivalent
- Identify external communication requirements based on laws and regulations. Work with internal staff (e.g., Legal) as required ensuring the appropriate communication is disseminated
- Ensure postmortem incident reviews are conducted as needed
- Communicate incident information with supervisors, resource owners, and Internal Audit as needed

Help Desk

- Receive and manage calls from users relating to security events or incidents
- Document information about the problem via the incident management system
- Resolve minor security events where standard operating processes exist (e.g., password reset, account unlock)
- Notify Security at the time a problem/event has escalated to a security incident
- Communicate to end users as directed for security incidents
- Maintain a knowledge base pertinent to security incidents
- Contact the Director - Facilities Management to initiate a police report for stolen/missing [ENTITY NAME] equipment

Incident Lead

The Security Analyst or other designee manages the overall response, recovery and communication activities for security incidents

Process:

- Respond to and investigate reported cyber security incidents
- Perform analysis regarding impact, cause, and restoration ensuring forensic data is captured before restoration takes place
- Determine resources necessary to work the cyber security incident (e.g., Technical Services, Desktop/Server Support Team, Security Team)

Communication:

- Notify the Director – Information Security or equivalent when the security incident is reportable, impacts more than one workstation, impacts an application or system, or results in a data breach
- Work with the Help Desk to prepare end user communication as needed

Classify and Report:

- Report Reportable Cyber or Physical Security Incidents to the Department of Energy (DOE) on Form OE-417 within one hour for emergency alerts and within

six hours for normal alerts. For further explanation, refer to Form OE-417:
  - Email: doehqeos@hq.doe.gov
  - Fax: 202-586-8485
  - Phone: 202-586-8100
- Send completed Form OE-417 to ES-ISAC at:
  - Email: esisac@esisac.com
  - Fax: 609-452-9550
  - Phone: 404-446-9780 (#2)

Documentation:

- Document cyber security incident information using the Information Security Incident Response Summary. (see example Figure 1**)**
- Send the completed electronic copy to the Director - Information Security
- Ensure the incident ticket in the incident management system is appropriately categorized
- Gather and secure documentation for NERC reportable cyber incidents

Support Staff

Support staff may be involved in a cyber security incident as directed by the Director In-Charge, Incident Lead, or Help Desk including Security, Energy Supply Engineering, Desktop/IT Technical Services Facilities Management, and Enterprise Systems

- Respond to and begin diagnosing cyber security events/incidents
- Analyze and contain the cyber security incident
- Upon approval from IT Security, eradicate the cause of the cyber security incident
- Recover affected computers/systems back to a normal status, after ensuring forensic information is captured

Report status updates to the [ENTITY NAME] Help Desk as needed.

Identified Roles and Responsibilities are documented in the Cyber Security Incident response plan

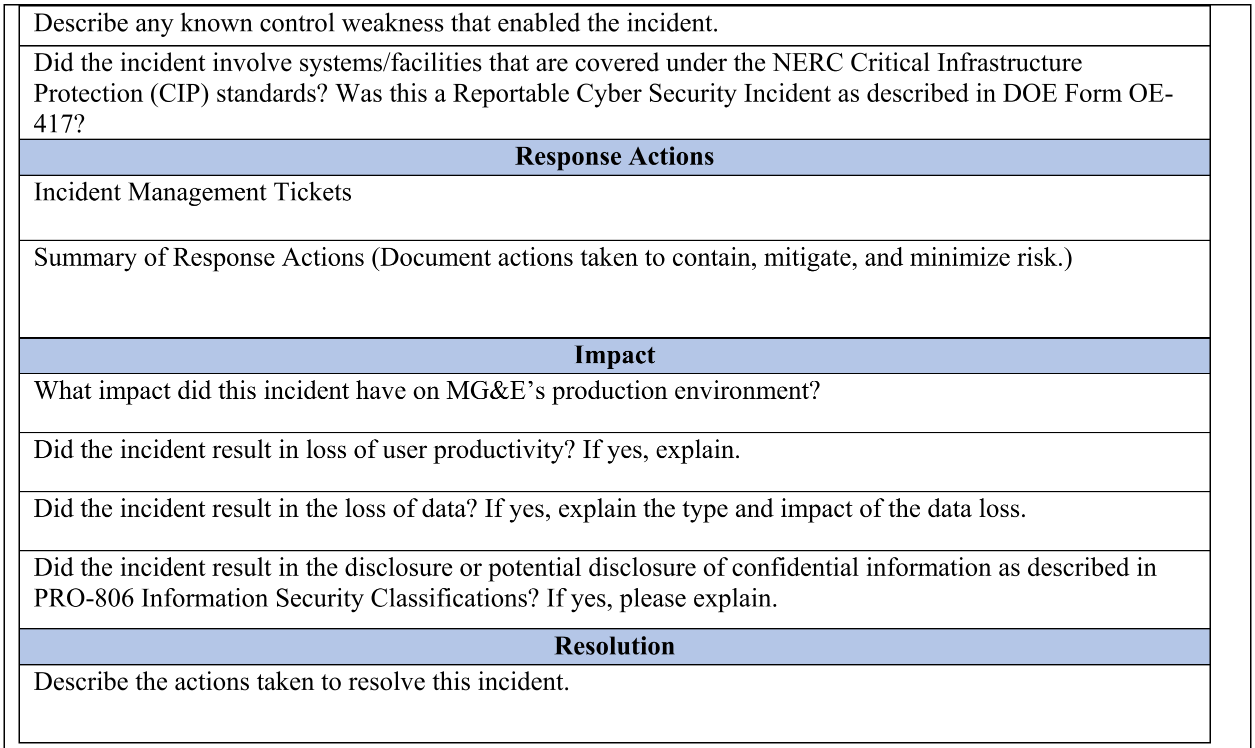
Incident Handling (Attachment 1, Section 4.4)

Application: Establish procedures incident handling procedures and employ them

Evidence: Document incident handling procedures in the plan and document the use of them

Information Security Incident Response Summary Form

INFORMATION SECURITY INCIDENT RESPONSE SUMMARY			
Incident Reporter Information			
Name			Date
Title		Location	
Phone/Contact Information		Lease Tag Number	
Incident Summary			
Type of Incident			
□Malware	□Phishing	□Denial of Service	□Procedure Violation
□Unauthorized Access	□Theft of Equipment	□Physical Security	□Other
Description of Incident			
Describe the root cause of the incident, for example, how did a computer get infected or how did an intruder gain access to a facility or system.			



Describe any known control weakness that enabled the incident.
Did the incident involve systems/facilities that are covered under the NERC Critical Infrastructure Protection (CIP) standards? Was this a Reportable Cyber Security Incident as described in DOE Form OE-417?
Response Actions
Incident Management Tickets
Summary of Response Actions (Document actions taken to contain, mitigate, and minimize risk.)
Impact
What impact did this incident have on MG&E's production environment?
Did the incident result in loss of user productivity? If yes, explain.
Did the incident result in the loss of data? If yes, explain the type and impact of the data loss.
Did the incident result in the disclosure or potential disclosure of confidential information as described in PRO-806 Information Security Classifications? If yes, please explain.
Resolution
Describe the actions taken to resolve this incident.

Forms can be used for documenting processes

Testing the Cyber Security Indent Response Plan (Attachment 1, Section 4.5)

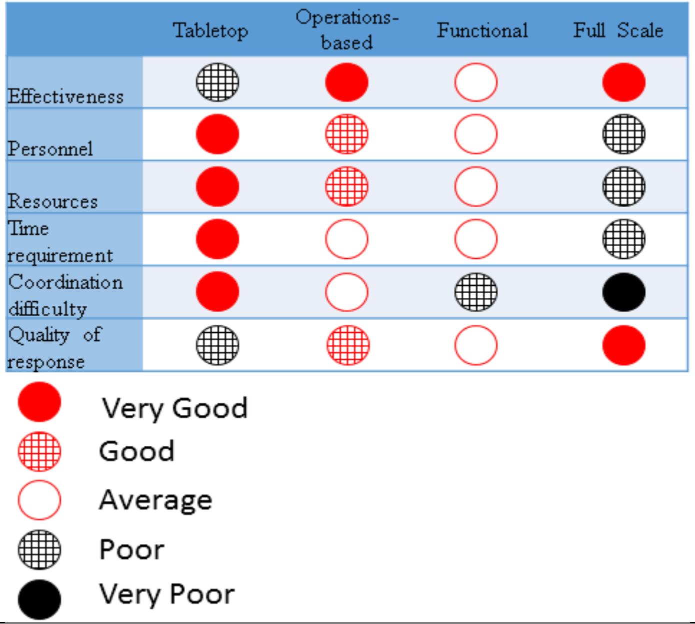
Application: Every 36 months the plan needs to be tested. Due to the time requirements, test evidence should be dated. Tests are critical for identifying strengths and deficiencies in the plan, and in training personnel. Tests can be conducted in a variety of ways such as:

- Tabletop Exercise (TTX): involves key personnel discussing simulated scenarios in an informal setting. TTXs can be used to assess plans, policies, and procedures
- Operations-based Exercise: validates plans, policies, agreements and procedures, clarify roles and responsibilities, and identify resource gaps in an operational environment
- Functional Exercise: examines and/or validates the coordination, command, and control between various coordination centers. A functional exercise does not involve any "boots on the ground"
- Full-Scale Exercise (FSE): a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional and "boots on the ground" response (e.g., firefighters decontaminating mock victims)
- Actual Incident: results from the handling of an actual Cyber Security Incident

Each test type has its benefits and detriments and focus on different results. Entities should select the test that best meets their intent.

Regardless of test chosen, evaluation criteria and parameters should be established prior to the test.

Table of Pros and Cons of Incident Response Plan Tests



	Tabletop	Operations-based	Functional	Full Scale
Effectiveness	▩	🔴	○	🔴
Personnel	🔴	▦	○	▩
Resources	🔴	▦	○	▩
Time requirement	🔴	○	○	▩
Coordination difficulty	🔴	○	▩	●
Quality of response	▩	▦	○	🔴

🔴	Very Good
▦	Good
○	Average
▩	Poor
●	Very Poor

The table shows pros and cons for methods of implementing Cyber Security Incident response plan tests

Evidence: Entities have a variety of options for providing evidence to document the plan was tested including:

- Dated summary of the test
- Dated compilation of notes, logs, and communication from the test
- Dated Lessons learned report

Updating the Cyber Security Incident Response Plan (Attachment 1, Section 4.6)

After a test or actual incident, the entity has 180 days to update the incident response plan if needed. It is important to update the plan to fix identified deficiencies and make improvements to optimize the plan. It is equally important to communicate the changes to personnel affected by or responsible for the changes.

Application: While there are multiple methods for changing an incident response plan after a test, one good method is doing an after action review. After action reviews cover the following questions:

- What was supposed to happen?
- What actually happened?
- Why were there differences?
- What worked?
- What didn't work?
- Why?
- What would you do differently next time?

After answering these questions, plans should be updated and training conducted to optimize the plan and response.

Evidence: Entities have multiple options for evidence including but not limited to the following:

- Dated documentation of post incident review meeting notes
- Dated lessons learned documents
- Dated notes identifying no lessons were learned
- Dated and revised Cyber Security Incident response plan showing changes based on lessons learned
- Dated emails, training sign-in sheets, distributions covering lessons learned

Considerations for Programs

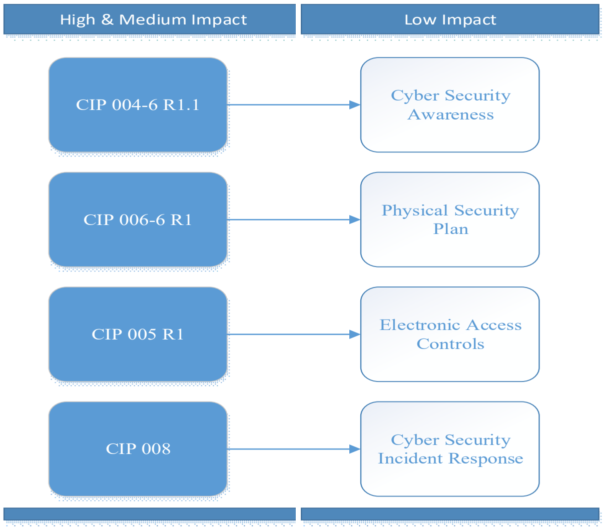
Simplicity

Keeping programs as simple as possible while meeting or exceeding the requirements has the following benefits:

- Easier to implement
- Easier to coordinate
- Easier to gain corporate and cultural acceptance
- Easier for employees to follow
- Easier for an auditor to understand
- Easier to find and fix issues
- Easier to manage
- Easier to update and change
- Easier to streamline decision-making
- Clarity
- Focus
- Effectiveness
- Adding complexity is easy, but maintaining simplicity is hard

Incorporating High and Medium BES Cyber Systems

Entities with low impact BES Cyber Systems as well as high or medium impact BES Cyber Systems may benefit from incorporating programs or procedures from used for those BES Cyber Systems.



Cooperation

Cooperation and coordination between business units helps prevent compartmentalized, duplicated, and/or non-uniform operations.

Benefits:

- Expert pool
- Decrease costs
- More efficient
- Easier to automate
- Flexible/reliable/contingency operations
- sustainability
- Visibility
- Improves security
- Measurability/benchmarking
- Technology Integration
- Growth
- Consistency
- Improved, consistent quality
- Increased employee safety
- Synergies
- Ease of management

Firm Foundation

CIP regulations provide a standard minimum level of security that is a firm foundation for a security program. It is good to implement security measures beyond the regulations but be sure to meet these requirements first.

High Water Mark

Entitles with BCAs with different impact ratings at a location, consideration should be made when defining logical boundaries. If different impact ratings are present on the same network, the higher requirements will need to be put in place for all devices. By segregating networks based on impact ratings, the entity would only be required to apply the controls for the appropriate level. Depending on the situation, it might be more practical to keep the devices on the same network and provide greater security controls than would otherwise be required.

Define Roles and Responsibilities

Defining roles and responsibilities takes an upfront investment in effort and time but will pay dividends. Defining roles removes wasteful ambiguity in planning and operations. In planning, it helps ensures all tasks are assigned and enables those responsible to help design programs. In operations, it efficiently allocates resources and ensures personnel are not overtasked. Defining responsibilities links responsible parties to tasks they need to accomplish and makes them accountable for their assigned tasks.

Fifteen Month Reoccurrences

Be aware that some requirements must be accomplished every fifteen months. It is possible to complete tasks every calendar year and still violate this timeline. If computer based training was performed on January 2017 and not accomplished until December 2018, the fifteen month requirement would not be met.

Management Practices

While not required, some management practices can help entities ensure tasks are being completed and documented as necessary. The following are a few examples of these management practices:

- Manager(s) creates, reviews, and approves lists associated with each requirement
- Formally document interpretations or rationale associated with each requirement
- Manager(s) or delegate(s) periodically spot checks implemented controls
- Manager(s) establishes an administrative process to address and verify mid-cycle changes to processes and documentation

Summary

This document intends to provide considerations and options to evaluate when determining an approach to protecting low impact BES Cyber Systems. Due to the open interpretation of these standards, diverging security objectives, and differences of systems and scenarios of each entity, this document does not provide a prescriptive guide. The wording of the Reliability Standards allows the freedom for to develop methods to efficiently and effectively meet security requirements based on the entities needs.

The physical and electronic access control requirements leave considerable room for interpretation, and it is important that entities adequately weigh the pros and cons before determining their solutions. Each entity should tailor solutions to best meet their objectives and consider the risk associated with the particular BES asset or low impact BES Cyber Systems. This approach differs from the prescriptive requirements for high impact and medium impact BES Cyber Systems.

The NERC CIP standards frequently change and adapt. At this time, there is an effort to develop CIP-003-7 impacting the implementation of required security controls prior to the required timeline. Entities should keep up to date on changes and consider them in their solutions, so new revisions do not cause unnecessary difficulties and costs.

The intent of the CIP standards is to improve reliability via providing security. A solid security program may lead to a secure cyber system with little adaptation or effort. Though application of the standards ensures a minimum level of protection and controls are in place, entities can benefit by building on this foundation to provide additional security measures for their systems where and when appropriate.

Appendix A – References

1. CIP-002-5.1 Cyber Security – BES Cyber System Categorization
2. CIP-003-6 Cyber Security – Security Management Controls
3. MRO Standards Committee Standard Application Guide CIP-002-5.1
4. NERC Glossary of Terms used in NERC Reliability Standards

Date	Revisions /Reviewed	Developed By
1/26/2017	Version 0	SMET
2/06/2017	Version 0.1 –Revised enforcement date R1.2	MRO Staff