« *Technical Rationale and Justification for Reliability Standard* » (Justification technique) et « *Implementation Guidance* » (Guide d'application) (version anglaise)

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT

Cyber Security – Electronic Security Perimeter(s)

Technical Rationale and Justification for Reliability Standard CIP-005-7

October 2020

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

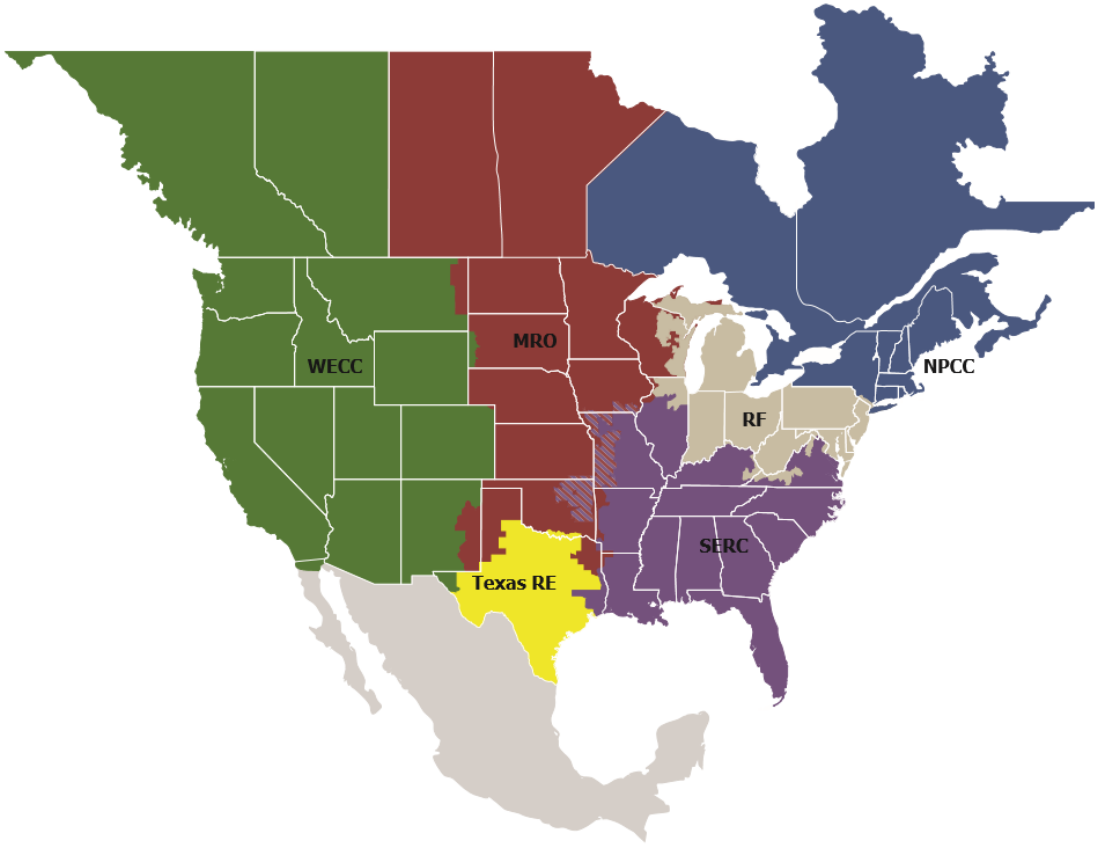
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-005-7. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-005-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in this Section that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Furthermore, Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of Bulk Electric System (BES) Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Updates to this document now include the Project 2019-03 – Cyber Security Supply Chain Risks Standard Drafting Team's (SDT's) intent in drafting changes to the requirements.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 850 on October 18, 2018, calling for modifications to the Supply Chain Suite of Standards to address Electronic Access Control or Monitoring Systems (EACMS), specifically those system that provide electronic access control or monitoring to high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT drafted Reliability Standard CIP-005-7 to require Responsible Entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

Additionally, the Project 2019-03 SDT removed Interchange Coordinator or Interchange Authority as that registration has been retired.

New and Modified Terms Used in NERC Reliability Standards

CIP-005-7 uses the following definition(s), which are cited below for reference when reading the technical rational that follows.

Proposed Modified Terms: None

Proposed New Terms: None

Requirement R1

General Considerations for Requirement R1

The Electronic Security Perimeter ("ESP") serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network-based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter."

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

Reference to prior version: (Part 1.1) CIP-005-4, R1

Change Rationale: (Part 1.1)
Explicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.

Reference to prior version: (Part 1.2) CIP-005-4, R1

Change Rationale: (Part 1.2)
Changed to refer to the defined term Electronic Access Point and BES Cyber System.

Reference to prior version: (Part 1.3) CIP-005-4, R2.1

Change Rationale: (Part 1.3)
Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.

Reference to prior version: (Part 1.4) CIP-005-4, R2.3

Change Rationale: (Part 1.4)
Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.

Reference to prior version: (Part 1.5) CIP-005-4, R1

Change Rationale: (Part 1.5)
Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Requirement 1

CIP-005-5, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The CIP Cyber Security Standards do not require network segmentation of BES Cyber Systems by impact classification. Many different impact classifications can be mixed within an ESP. However, all of the Cyber Assets and BES Cyber Systems within the ESP must be protected at the level of the highest impact BES Cyber System present in the ESP (i.e., the "high water mark") where the term "Protected Cyber Assets" is used. The CIP Cyber Security Standards accomplish the "high water mark" by associating all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, then each Cyber Asset of the low impact BES Cyber System are "Associated Protected Cyber Assets" of the high impact BES Cyber System and must meet all the requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero-day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communication to that known range. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rouge connections can be detected and blocked.

This requirement applies only to communications for which access lists and 'deny by default' type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run between two Cyber Assets. Without a clear 'perimeter type' security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions ("TFEs") rather than increased security.

As for dial-up connectivity, the Standard Drafting Team's intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. If the dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Requirement R2

General Considerations for Requirement R2

Registered Entities use Interactive Remote Access to access Cyber Assets to support and maintain control systems networks. Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements are in effect for management of secure remote access to Cyber Assets to be afforded the NERC CIP protective measures. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences. Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources should only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

The Intermediate System serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed to connect to Cyber Assets within the Electronic Security Perimeter directly. The use of an Intermediate System also protects the Cyber Asset from vulnerabilities on the remote computer.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords.
But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

Encryption is used to protect the data that is sent between the remote computer and the Intermediate System. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. This is especially important when using the Internet as the communication means.

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.1) New

Change Rationale: (Part 2.1)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.2) CIP-007-5, R3.1

Change Rationale: (Part 2.2)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The purpose of this part is to protect the confidentiality and integrity of each Interactive Remote Access session.

Reference to prior version: (Part 2.3) CIP-007-5, R3.2

Change Rationale: (Part 2.3)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.

Requirement R3

Requirement Part 3.1 and Part 3.2 Vendor Remote Access Management for EACMS and PACS

The 2019-03 SDT added Requirement R3 to contain the requirements for all types of vendor remote access management for EACMS and PACS (i.e. system to system, user to system). EACMS were added based on FERC order 850 paragraph 5 where FERC ordered NERC to create a drafting team to add these devices. EACMS were added based on the risks FERC noted in paragraph 4, where a Department of Homeland Security Industrial Control System-Cyber Emergency Response Team (DHS ICS-CERT) said firewalls (normally defined as an EACMS) is the "first line of defense within an Industry Control System (ICS) network environment". The compromise of those devices that control access management could provide an outsider the "keys to the front door" of the ESP where BES Cyber Systems reside. An intruder holding the "keys to the front door" could use those "keys" to enter the ESP or modify the access controls to allow others to bypass authorization.

In Requirement R3 Part 3.1 and Part 3.2, the word "connection" is the mechanism for a user or a system to interact with an EAMCS or PACS for the purpose of authenticating.

In Requirement R3 Part 3.1 and Part 3.2, the word "authenticate" is the mechanism for the EACMS or PACS to identify the user or device. This permits the EACMS or PACS to first perform its function to authenticate the user or device that is connecting, which in turn permits the entity to delineate or differentiate vendor-initiated connections from other remote access connections. This new proposed language is not prescriptive as to how authentication must occur to permit administrative and technical methods.

In Requirement R3 Part 3.2, the word "control" provides the entity flexibility to allow the vendor to reconnect under a specific set of conditions, established by the entity, where the reconnection is necessary to support critical operations of the entity. If the entity determines that they do not want to allow or does not need to allow a reconnection they can employ means to stop any reconnection.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Since remotely compromised PACS still require physical presence to exploit BES Cyber Systems, the SDT conducted extensive dialogue and considerations for the addition of PACS. The SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warranted their inclusion as an applicable Cyber Asset. Further, the inclusion of PACS:

1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",
2. addresses the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and

3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "*Cyber Security Supply Chain Risks"*[1].

NERC's final report on "*Cyber Security Supply Chain Risks"*, states on page 4, "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." PACS are intended to manage physical threats to BES Cyber Systems, thus protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

Additionally, NERC states on page 15 of their final report on "*Cyber Security Supply Chain Risks"* that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical accesses or monitoring controls that have not been compromised in order to gain access." While a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it could demonstrate a threat Actor's intention to gain fully unauthorized electronic access.

While other Reliability Standards mitigate certain security risks relating to PACS none address supply chain risk. Based on this analysis the SDT included PACS within the applicable section of both Requirement Parts 3.1 and 3.2.

An additional aspect of the NERC Supply Chain Report, the SDT considered was the risk associated with the access control vs. access monitoring functions of both EACMS and PACS. While both types of systems, under the current definitions, have various functional activities they perform, the NERC Supply Chain Report pointed to the increased risk of the access control function beyond the access monitoring function. The SDT considered limiting the scope of the requirements to only those access control functions, however chose to stay with the currently approved definition of both EACMS and PACS. The SDT concluded staying with approved definitions would introduce less confusion. Additionally, an attempt to change the EACMS and PACS definition was outside the 2019-03 SAR.

Entities may or may not allow remote access into any of its systems, (BES Cyber Systems, EACMS or PACS), however if remote access is allowed, options to determine remote access connection(s) and capability to disable remote access connection(s) is required.

[1] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

Technical Rational for Reliability Standard CIP-005-6

This section contains a "cut and paste" of the Technical Rationale components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-005-6 standard to preserve any historical references. Similarly, former GTB content providing compliance guidance can be found in a separate Implementation Guidance document for this standard.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Furthermore, Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

CIP-005-5, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The CIP Cyber Security Standards do not require network segmentation of BES Cyber Systems by impact classification. Many different impact classifications can be mixed within an ESP. However, all of the Cyber Assets and BES Cyber Systems within the ESP must be protected at the level of the highest impact BES Cyber System present in the ESP (i.e., the "high water mark") where the term "Protected Cyber Assets" is used. The CIP Cyber Security Standards accomplish the "high water mark" by associating all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, each Cyber Asset of the low impact BES Cyber System is an "Associated Protected Cyber Asset" of the high impact BES Cyber System and must meet all requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP.

Responsible Entities should know what traffic needs to cross an EAP and document those reasons to ensure the EAPs limit the traffic to only those known communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

The EAP

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate, and large ranges of internal addresses may be allowed. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity's address space. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked.

This requirement applies only to communications for which access lists and 'deny by default' type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run between two Cyber Assets. Without a clear 'perimeter type' security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions ("TFEs") rather than increased security.

As for dial-up connectivity, the Standard Drafting Team's intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. If the dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Requirement R2:

See Secure Remote Access Reference Document (see remote access alert).

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

The Electronic Security Perimeter ("ESP") serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter."

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

Reference to prior version: (Part 1.1) CIP-005-4, R1

Change Rationale: (Part 1.1)
E*xplicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.*

Reference to prior version: (Part 1.2) CIP-005-4, R1

Change Rationale: (Part 1.2)
Changed to refer to the defined term Electronic Access Point and BES Cyber System.

Reference to prior version: (Part 1.3) CIP-005-4, R2.1

Change Rationale: (Part 1.3)
Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.

Reference to prior version: (Part 1.4) CIP-005-4, R2.3

Change Rationale: (Part 1.4)
Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.

Reference to prior version: (Part 1.5) CIP-005-4, R1

Change Rationale: (Part 1.5)
Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Rationale for R2:

Registered Entities use Interactive Remote Access to access Cyber Assets to support and maintain control systems networks. Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements are in effect for management of secure remote access to Cyber Assets to be afforded the NERC CIP protective measures. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences. Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources will only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

The Intermediate System serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed to connect to Cyber Assets within the Electronic Security Perimeter directly. The use of an Intermediate System also protects the Cyber Asset from vulnerabilities on the remote computer.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords.
But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

Encryption is used to protect the data that is sent between the remote computer and the Intermediate System. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. This is especially important when using the Internet as the communication means.

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.1) New

Change Rationale: (Part 2.1)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.2) CIP-007-5, R3.1

Change Rationale: (Part 2.2)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The purpose of this part is to protect the confidentiality and integrity of each Interactive Remote Access session.

Reference to prior version: (Part 2.3) CIP-007-5, R3.2

Change Rationale: (Part 2.3)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.

Change Rationale: (Part 2.4 and 2.5)
Requirement R2 Parts 2.4 and 2.5 addresses Order No. 829 directives for controls on vendor-initiated remote access to BES Cyber Systems covering both user-initiated and machine-to machine vendor remote access (P. 51). The objective is to mitigate potential risks of a compromise at a vendor during an active remote access session with a Responsible Entity from impacting the BES.

The objective of Requirement R2 Part 2.4 is for entities to have visibility of active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) that are taking place on their system. This scope covers all remote access sessions with vendors. The obligation in Part 2.4 requires entities to have a method to determine active vendor remote access sessions. While not required, a solution that identifies all active remote access sessions, regardless of whether they originate from a vendor, would meet the intent of this requirement. The objective of Requirement R2 Part 2.5 is for entities to have the ability to disable active remote access sessions in the event of a system breach as specified in Order No. 829 (P. 52).

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT Implementation Guidance pending submittal for ERO Enterprise Endorsement

DRAFT

Cyber Security – Electronic Security Perimeter(s)

Implementation Guidance for Reliability Standard CIP-005-7

October 2020

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

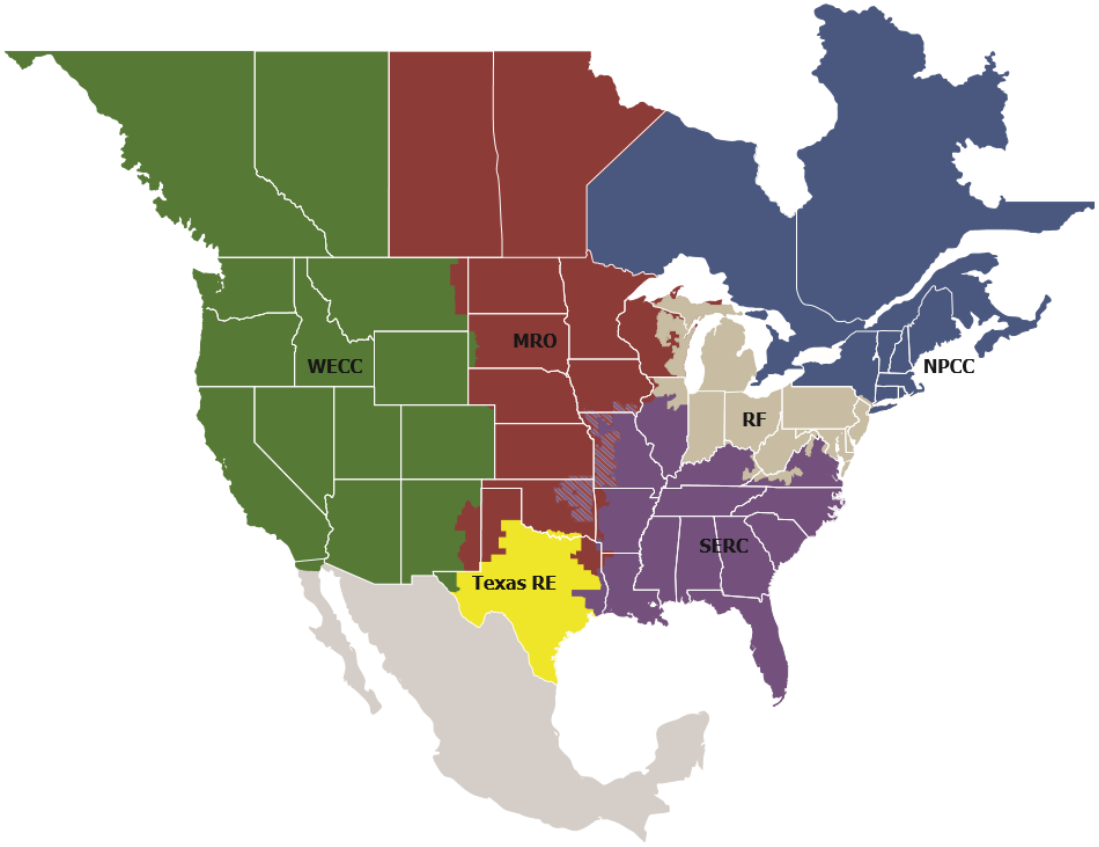
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

The Standards Project 2019-03 – Cyber Security Supply Chain Risks Standards Drafting Team (SDT) prepared this Implementation Guidance to provide example approaches for compliance with the modifications to CIP-005-7. Implementation Guidance does not prescribe the only approach but highlights one or more approaches that could be effective in achieving compliance with the standard. Because Implementation Guidance only provides examples, entities may choose alternative approaches that better fit their individual situations.[1] This Implementation Guidance for CIP-005-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Responsible entities may find it useful to consider this Implementation Guidance document along with the additional context and background provided in the SDT-developed Technical Rationale and Justification for the modifications to CIP-005-7.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 850 on October 18, 2018, calling for modifications to the Supply Chain Suite of Standards to address Electronic Access Control or Monitoring Systems (EACMS), specifically those systems that provide electronic access control or monitoring to high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT drafted Reliability Standard CIP-005-7 to require responsible entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

[1] NERC's Compliance Guidance Policy

Requirement R3

The 2019-03 SDT added Requirement 3 Vendor Remote Access Management for EACMS and PACS and created new Requirements Parts 3.1 and 3.2 to meet FERC order 850 and the NERC Supply Chain Risk report. If an entity allows remote access to their EACMS and PACS the method to determine authenticated vendor-initiated remote connections is documented and the ability to disable that remote connection is required. For example, if an entity utilizes its corporate remote access solution to allow remote connection into its PACS, the entity would need to document the authenticated remote connection method and develop a process to terminate such connections after authentication. Some examples of how an entity might terminate these connections may be as simple as, but are not limited to actions like disabling a token or certificate for a vendor account(s), suspending or deleting the vendor account(s) in Active Directory, blocking the vendor's IP range, or physically disconnecting a network cable.

Intermediate Systems (a subset of EACMS) use is not a requirement for remote access to other EACMS, lessening the potential of the recursive requirement ("hall of mirrors") However, if an Entity uses the same system (Intermediate System for example) for remote connections and access into both their BES Cyber Systems and their EACMS (within the Electronic Security Perimeter), the process of terminating vendor-initiated remote connections begins after the entity has determined, through authentication, that this particular connection attempt should not be allowed. For this example, assume the Entity is using a jump host as its Intermediate System with multifactor and Active Directory authentication. When the vendor attempts the remote access connection, the jump host will present both the Active Directory login screen as well as the multifactor access portal. The Entity could choose to disable the Active Directory account, disable the multifactor account or both. Any of those methods disable the vendor's ability to make a connection. The remote access vendor will attempt to "connect" with the EACMS however, after unsuccessful authentication the connection attempt will be terminated. This scenario illustrates a method to disallow vendor-initiated remote access while eliminating the recursive requirements ("hall of mirror") issue.

Where an entity strictly prohibits vendor-initiated remote access as a function of policy, the entity should consider the following to provide reasonable assurance of conformance to that policy, noting the policy itself can become the documented method:

1. Document whether the policy contains provisions to allow deviations to accommodate emergency situations, as well as the process to handle or approve those policy deviations, and how vendor-initiated remote connection termination would be handled if needed during those emergencies.
2. An Entity could identify internal controls to periodically verify vendor-initiated remote access is prohibited within system configurations. Some examples may include, but are not limited to:
    a. Leveraging periodic access reviews conducted in support of CIP-004-6 Requirement R4 and CIP-007-6 Requirement R5 to provide ongoing reasonable assurance that vendor-initiated remote access is prohibited as expected.
    b. Leveraging periodic inventory reviews that may be associated to annual CIP-002-5.1a Requirement R2 to assess BES Cyber System classifications and network topologies to provide supporting records that vendor-initiated remote access needs and configurations were reviewed and confirmed to be in alignment with policy expectations.
    c. Leveraging periodic rule set or access list configuration reviews that may be performed in support of CIP-005-7 and verification of implemented controls for EAP, ESP, and as Intermediate System implementation to provide additional assurance that vendor-initiated remote access is prohibited as expected.
    d. Leveraging periodic configuration change management reviews performed in support of CIP-010-4 Requirement R2 to assess BES Cyber Systems and unexpected (or potentially unauthorized) changes

to baseline configurations that could lead to the introduction of vendor-initiated remote access to provide additional assurance that vendor-initiated remote access is prohibited as expected.

e. Leveraging periodic cyber vulnerability assessments performed in support of CIP-010-4 Requirement R3 to assess BES Cyber System connectivity characteristics, interface and protocol configurations, and unexpected (or potentially unauthorized) physical connections to provide additional assurance that vendor-initiated remote access is prohibited as expected.

f. Provisions within the Responsible Entity's remote access management program or processes detailing internal controls and technology used to monitor for unauthorized access to provide additional assurance that the introduction of vendor-initiated remote access could be detected and reverted/revoked if established in violation of policy.

Staff augmentation presents another example of vendor remote access; however, this method provides less risk as other vendor remote access. The process involved requires an entity to complete all the CIP-004 tasks for the vendor in the same rigor as with an employee (training, PRA, etc.) and provide the vendor with an entity managed device to facilitate the remote access. This type of vendor remote access should be managed the same as an entity manages employee remote access.

Implementation Guidance for CIP-005-6

This section contains a "cut and paste" of the Implementation Guidance components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-005-6 standard to preserve any historical references. Similarly, former GTB content providing SDT intent and technical rationale can be found in a separate Technical Rational document for this standard.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Requirement R1:

Responsible Entities should know what traffic needs to cross an EAP and document those reasons to ensure the EAPs limit the traffic to only those known communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate, and large ranges of internal addresses may be allowed. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity's address space. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked

Some examples of acceptable methods include dial-back modems, modems that must be remotely enabled or powered up, and modems that are only powered on by onsite personnel when needed along with policy that states they are disabled after use.

Technologies meeting this requirement include Intrusion Detection or Intrusion Prevention Systems (IDS/IPS) or other forms of deep packet inspection. These technologies go beyond source/destination/port rule sets and thus provide another distinct security measure at the ESP.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT

Cyber Security — Configuration Change Management and Vulnerability Assessments

Technical Rationale and Justification for Reliability Standard CIP-010-4

October 2020

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

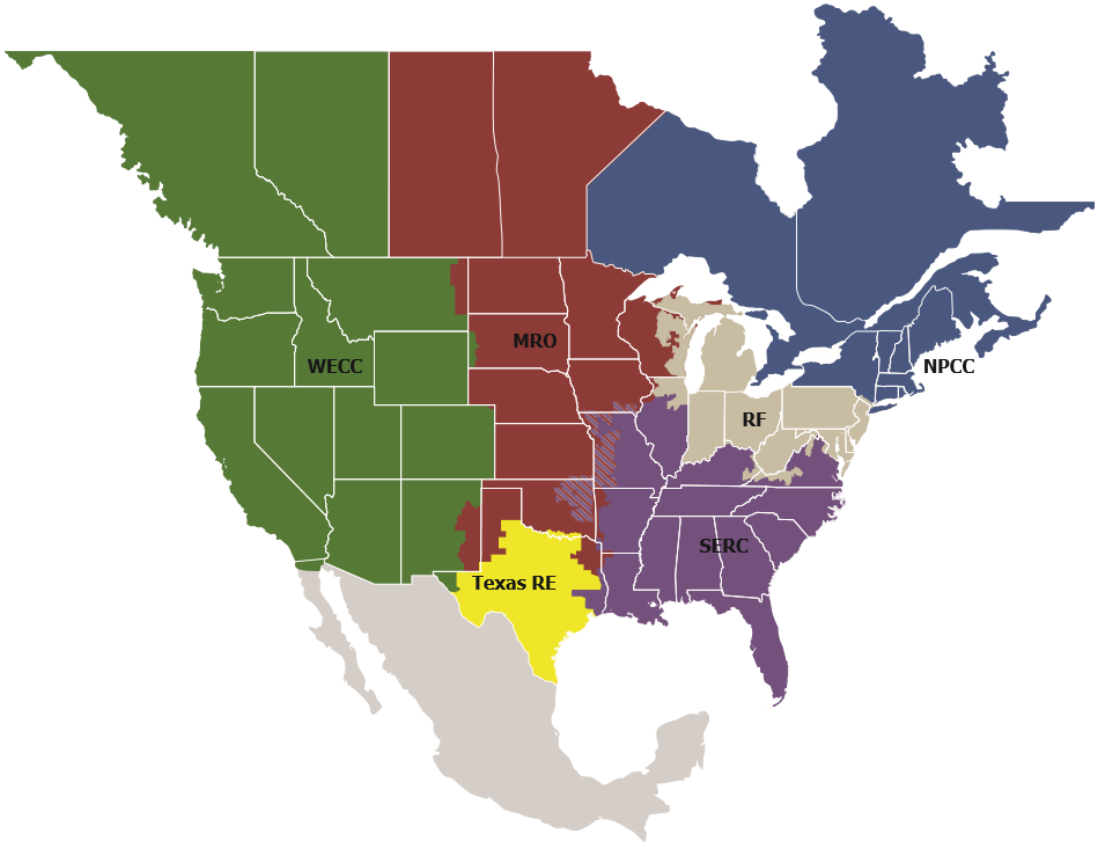
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-010-4. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justification for CIP-010-4 is not a Reliability Standard and should not be considered mandatory and enforceable.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 850[1] on October 18, 2018, calling for modifications to the Supply Chain Suite of Standards, in which the summary on page 1 states, "…the Commission directs NERC to develop and submit modifications to the supply chain risk management Reliability Standards so that the scope of the Reliability Standards include Electronic Access Control and Monitoring Systems." In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report, Staff Report and Recommended Actions[2], to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT drafted Reliability Standard CIP-010-4 to require responsible entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

[1] https://www.ferc.gov/whats-new/comm-meet/2018/101818/E-1.pdf

[2] https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

New and Modified Terms Used on NERC Reliability Standards

CIP-010-4 uses the following definition(s), which are cited below for reference when reading the technical rational that follows.

Proposed Modified Terms: None

Proposed New Terms: None

Requirement R1

General Considerations for Requirement R1

FERC Order 850, Paragraph 5 and Paragraph 30 directed modifications to Reliability Standard CIP-010-3 Requirement R1 to address supply chain risk management for Electronic Access Control or Monitoring Systems (EACMS) for high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards to address PACS that provide physical access control (excluding alarming and logging) to high and medium impact BES Cyber Systems, and modifications were addressed by the 2019-03 SDT.

Rationale for Requirement R1

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

Requirement R1 Part 1.6 addresses directives in Order No. 829 for verifying software integrity and authenticity prior to installation in BES Cyber Systems (P. 48). The objective of verifying software integrity and authenticity is to ensure that the software being installed in the BES Cyber System was not modified without the awareness of the software supplier and is not counterfeit.

Requirement R1 Part 1.6 addresses directives in Order No. 850 for verifying software integrity and authenticity prior to installation of an EACMS (P. 5 and P.30), and PACS from the NERC Cyber Security Supply Chain Risk Report[3] recommendation. The objective of verifying software integrity and authenticity is to ensure that the software being installed on EACMS and PACS was not modified without the awareness of the software supplier and is not counterfeit.

Due to the nature of PACS and the potential need for physical presence, the SDT conducted extensive dialogue and consideration for the addition of PACS to the requirements, the SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warrants the inclusion of PACS as an applicable Cyber Asset category for supply chain risk management controls. Further, the inclusion of PACS:

1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",
2. is consistent with the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and
3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "*Cyber Security Supply Chain Risks"*[4].

In further support of the SDT's decision to include PACS, as cited on page 4 of NERC's final report on "*Cyber Security Supply Chain Risks"*, "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." While this statement appears in the context of EACMS, it acknowledges physical security threats equally; therefore, the concept is transferable and applicable to PACS, which serve as an integral component to a strategy involving layers of detective and preventive security controls. PACS are intended to manage physical access to BES Cyber Systems in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES and are implemented with that specific intention to protect the BES Cyber System.

[3] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

[4] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

Additionally, NERC states on page 15 of their final report on "*Cyber Security Supply Chain Risks"* that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical access or monitoring controls that have not been compromised in order to gain access." While it might be a fair point that a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it stands to reason that a threat actor's intention to gain unauthorized electronic access to a PACS does so 1) with the knowledge of it being an initial deliberate action to facilitate undetected reconnaissance, and 2) further undetected methodical compromise and intentional harm to the BES Cyber Systems the PACS is intended to protect.

Furthermore, a precedent is set in CIP-006-6 Requirement R1 Part 1.5 that recognizes the importance of PACS, its functions, and the timeliness of information provided by these systems by requiring issuance of an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter (PSP) to incident response personnel within 15 minutes of detection. This strict timeline suggests that compromised physical security poses an imminent threat to the associated BES Cyber System and the reliable operation of the BES Facilities it serves.

The SDT agrees that NERC correctly refers to various Reliability Standards that mitigate certain security risks relating to PACS; however, the SDT asserts that these existing requirements do not address risk associated to the supply chain and therefore do not sufficiently mitigate that risk.

An additional aspect of the NERC Supply Chain Report, the SDT risks associated with the different aspects of both EACMS and PACS. The NERC Supply Chain Report pointed to the increased risk of the control portion of both EACMS and PACS, and the SDT considered limiting the scope of the requirements to only those EACMS and PACS that perform the control functions. However, since the current approved definitions includes both control and monitoring for EACMS and control, logging and alerting for PACS, the SDT concluded it would introduce less confusion by referring to the authoritative term. The SDT did not attempt a change in definition due to the wide spread use of both EACMS and PACS within all the standards, and did not have authorization within its SAR to modify all of those standards.

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the

cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The language for use of a testing environment for deviations from baseline configuration was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly.

Software Verification

The concept of verifying the identity of the software source and the integrity of the software obtained from the software source helps prevent the introduction of malware or counterfeit software. This reduces the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System. The SDT intends for Responsible Entities to provide controls for verifying the baseline elements updated by vendors. It is important to note that this is not limited to only security patches.

Requirement R2

Rationale for Requirement R2

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

Baseline Monitoring

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible

Requirement R3

Rationale for Requirement R3

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

Vulnerability Assessments

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

Requirement R4

Rationale for Requirement R4

Requirement R4 responds to the directive in FERC Order No. 791, at Paragraphs 6 and 136, to address security-related issues associated with Transient Cyber Assets and Removable Media used on a temporary basis for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To mitigate the risks associated with such tools, Requirement R4 was developed to accomplish the following security objectives:

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.
- Requirement R4 incorporates the concepts from other CIP requirements in CIP-010-2 and CIP-007-6 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes

All requirements related to Transient Cyber Assets and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes.

Transient Cyber Assets and Removable Media

Because most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a plan for how they will manage the use of Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets and Removable Media are those devices connected temporarily to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Transient Cyber Assets and Removable Media do not provide BES reliability services and are not part of the BES Cyber Asset to which they are connected.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

While the definitions of Transient Cyber Asset and Removable Media include a conditional provision that requires them to be connected for 30 days or less, Section 1.1 of Attachment 1 allows the Responsible Entity to include provisions in its plan(s) that allow continuous or on-demand treatment and application of controls independent of the connected state. Please note that for on-demand treatment, the requirements only apply when Transient Cyber Assets and Removable Media are being connected to a BES Cyber System or Protected Cyber Asset. Once the transient

device is disconnected, the requirements listed herein are not applicable until that Transient Cyber Asset or Removable Media is to be reconnected to the BES Cyber Asset or Protected Cyber Asset.

The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type, ownership, and management.
With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity manages or reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity.

Vulnerability Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in the sections in Attachment 1 to address the risks posed by malicious code, software vulnerabilities, and unauthorized use when connecting Transient Cyber Assets and Removable Media. Mitigation in this context does not require that each vulnerability is individually addressed or remediated, as many may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is meant to reduce security risks presented by connecting the Transient Cyber Asset.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of “per Transient Cyber Asset capability” is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Attachment 1

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.1: Entities have a high level of control for the assets that they manage. The requirements listed herein allow entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection or use a combination of these methods. The devices may be managed individually or by group.

Section 1.2: Entities are to document and implement their process(es) to authorize the use of Transient Cyber Assets for which they have direct management. The Transient Cyber Assets may be listed individually or by asset type.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

The attachment also recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsible Entity. However, this does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and to meet their obligations.

Section 2.3: Determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity. The intent of this section is to ensure that after conducting the selected review from Sections 2.1 and 2.2, if there are deficiencies that do not meet the Responsible Entity's security posture, the other party is required to complete the mitigations prior to connecting their devices to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 3.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The entities must use the method(s) to detect malicious code on Removable Media before it is connected to the BES Cyber Asset. The timing dictated and documented in the entity's plan should reduce the risk of introducing malicious code to the BES Cyber Asset or Protected Cyber Asset.

For Section 3.2.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System or Protected Cyber Asset.

Technical Rationale for Reliability Standard CIP-010-3

This section contains a "cut and paste" of the Technical Rationale components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-010-3 standard to preserve any historical references. Similarly, former GTB content providing compliance guidance can be found in a separate Implementation Guidance document for this standard.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards:

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to "model" the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly.

Software Verification

The concept of software verification (verifying the identity of the software source and the integrity of the software obtained from the software source) is a key control in preventing the introduction of malware or counterfeit software. This objective is intended to reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System. The intent of the SDT is for Responsible Entities to provide controls for verifying the baseline elements that are updated by vendors. It is important to note that this is not limited to only security patches.

Requirement R2:

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible. For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

Requirement R4:

Because most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a plan for how they will manage the use of Transient Cyber Assets and Removable Media. The approach of defining

a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets and Removable Media are those devices connected temporarily to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Transient Cyber Assets and Removable Media do not provide BES reliability services and are not part of the BES Cyber Asset to which they are connected.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

While the definitions of Transient Cyber Asset and Removable Media include a conditional provision that requires them to be connected for 30 days or less, Section 1.1 of Attachment 1 allows the Responsible Entity to include provisions in its plan(s) that allow continuous or on-demand treatment and application of controls independent of the connected state. Please note that for on-demand treatment, the requirements only apply when Transient Cyber Assets and Removable Media are being connected to a BES Cyber System or Protected Cyber Asset. Once the transient device is disconnected, the requirements listed herein are not applicable until that Transient Cyber Asset or Removable Media is to be reconnected to the BES Cyber Asset or Protected Cyber Asset.

The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type, ownership, and management.

With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity manages or reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset, BES Cyber Asset, or Protected Cyber Asset.

Vulnerability Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in the sections in Attachment 1 to address the risks posed by malicious code, software vulnerabilities, and unauthorized use when connecting Transient Cyber Assets and Removable Media. Mitigation in this context does not require that each vulnerability is individually addressed or remediated, as many may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is meant to reduce security risks presented by connecting the Transient Cyber Asset.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of “per Transient Cyber Asset capability” is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example,, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.1: Entities have a high level of control for the assets that they manage. The requirements listed herein allow entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection or use a combination of these methods. The devices may be managed individually or by group.

Section 1.2: Entities are to document and implement their process(es) to authorize the use of Transient Cyber Assets for which they have direct management. The Transient Cyber Assets may be listed individually or by asset type. To meet this requirement part, the entity is to document the following:

1.2.1 User(s), individually or by group/role, allowed to use the Transient Cyber Asset(s). This can be done by listing a specific person, department, or job function. Caution: consider whether these user(s) must also have authorized electronic access to the applicable system in accordance with CIP-004.

1.2.2 Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group of locations.

1.2.3 The intended or approved use of each individual, type, or group of Transient Cyber Asset. This should also include the software or application packages that are authorized with the purpose of performing defined business functions or tasks (e.g., used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes), and approved network interfaces (e.g., wireless, including near field communication or Bluetooth, and wired connections). Activities, and software or application packages, not specifically listed as acceptable should be considered as prohibited. It may be beneficial to educate individuals through the CIP-004 Security Awareness Program and Cyber Security Training Program about authorized and unauthorized activities or uses (e.g., using the device to browse the Internet or to check email or using the device to access wireless networks in hotels or retail locations).

Section 1.3: Entities are to document and implement their process(es) to mitigate software vulnerabilities posed by unpatched software through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. Recognizing there is a huge diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in software vulnerability management solutions, options are listed that include the alternative for the entity to use a technology or process that effectively mitigates vulnerabilities.

- Security patching, including manual or managed updates provides flexibility to the Responsible Entity to determine how its Transient Cyber Asset(s) will be used. It is possible for an entity to have its Transient Cyber Asset be part of an enterprise patch process and receive security patches on a regular schedule or the entity can verify and apply security patches prior to connecting the Transient Cyber Asset to an applicable Cyber Asset. Unlike CIP-007, Requirement R2, there is no expectation of creating dated mitigation plans or other documentation other than what is necessary to identify that the Transient Cyber Asset is receiving appropriate security patches.
- Live operating system and software executable only from read-only media is provided to allow a protected operating system that cannot be modified to deliver malicious software. When entities are creating custom live operating systems, they should check the image during the build to ensure that there is not malicious software on the image.
- System hardening, also called operating system hardening, helps minimize security vulnerabilities by removing all non-essential software programs and utilities and only installing the bare necessities that the computer needs to function. While other programs may provide useful features, they can provide "back-door" access to the system, and should be removed to harden the system.

- When selecting to use other methods that mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet the software vulnerability mitigation objective.

Section 1.4: Entities are to document and implement their process(es) to mitigate malicious code through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. As with vulnerability management, there is diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in malicious code protections. When addressing malicious code protection, the Responsible Entity should address methods deployed to deter, detect, or prevent malicious code. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility just as with security patching, to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the opportunity that malicious software could become resident, much less propagate, from the Transient Cyber Asset to the BES Cyber Asset or BES Cyber System.
- Restricted communication to limit the exchange of data to only the Transient Cyber Asset and the Cyber Assets to which it is connected by restricting or disabling serial or network (including wireless) communications on a managed Transient Cyber Asset can be used to minimize the opportunity to introduce malicious code onto the Transient Cyber Asset while it is not connected to BES Cyber Systems. This renders the device unable to communicate with devices other than the one to which it is connected.
- When selecting to use other methods that mitigate the introduction of malicious code to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the introduction of malicious code objective.

Section 1.5: Entities are to document and implement their process(es) to protect and evaluate Transient Cyber Assets to ensure they mitigate the risks that unauthorized use of the Transient Cyber Asset may present to the BES Cyber System. The concern addressed by this section is the possibility that the Transient Cyber Asset could be tampered with, or exposed to malware, while not in active use by an authorized person. Physical security of the Transient Cyber Asset is certainly a control that will mitigate this risk, but other tools and techniques are also available. The bulleted list of example protections provides some suggested alternatives.

- For restricted physical access, the intent is that the Transient Cyber Asset is maintained within a Physical Security Perimeter or other physical location or enclosure that uses physical access controls to protect the Transient Cyber Asset.
- Full disk encryption with authentication is an option that can be employed to protect a Transient Cyber Asset from unauthorized use. However, it is important that authentication be required to decrypt the device. For example, pre-boot authentication, or power-on authentication, provides a secure, tamper-proof environment external to the operating system as a trusted authentication layer. Authentication prevents data from being read from the hard disk until the user has confirmed they have the correct password or other credentials. By performing the authentication prior to the system decrypting and booting, the risk that an unauthorized person may manipulate the Transient Cyber Asset is mitigated.

- Multi-factor authentication is used to ensure the identity of the person accessing the device. Multi-factor authentication also mitigates the risk that an unauthorized person may manipulate the Transient Cyber Asset.
- In addition to authentication and pure physical security methods, other alternatives are available that an entity may choose to employ. Certain theft recovery solutions can be used to locate the Transient Cyber Asset, detect access, remotely wipe, and lockout the system, thereby mitigating the potential threat from unauthorized use if the Transient Cyber Asset was later connected to a BES Cyber Asset. Other low tech solutions may also be effective to mitigate the risk of using a maliciously-manipulated Transient Cyber Asset, such as tamper evident tags or seals, and executing procedural controls to verify the integrity of the tamper evident tag or seal prior to use.
- When selecting to use other methods that mitigate the risk of unauthorized use to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the risk of unauthorized use objective.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

The attachment also recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsible Entity. However, this does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and to meet their obligations.

Section 2.1: Entities are to document and implement their process(es) to mitigate software vulnerabilities through the use of one or more of the protective measures listed.

- Conduct a review of the Transient Cyber Asset managed by a party other than the Responsible Entity to determine whether the security patch level of the device is adequate to mitigate the risk of software vulnerabilities before connecting the Transient Cyber Asset to an applicable system.
- Conduct a review of the other party's security patching process. This can be done either at the time of contracting but no later than prior to connecting the Transient Cyber Asset to an applicable system. Just as with reviewing the security patch level of the device, selecting to use this approach aims to ensure that the Responsible Entity has mitigated the risk of software vulnerabilities to applicable systems.
- Conduct a review of other processes that the other party uses to mitigate the risk of software vulnerabilities. This can be reviewing system hardening, application whitelisting, virtual machines, etc.
- When selecting to use other methods to mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet mitigation of the risk of software vulnerabilities.

Section 2.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.

- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This will limit the chance of introducing malicious software to an applicable system.

Section 2.3: Determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity. The intent of this section is to ensure that after conducting the selected review from Sections 2.1 and 2.2, if there are deficiencies that do not meet the Responsible Entity's security posture, the other party is required to complete the mitigations prior to connecting their devices to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 3.1: Entities are to document and implement their process(es) to authorize the use of Removable Media. The Removable Media may be listed individually or by type.

- Document the user(s), individually or by group/role, allowed to use the Removable Media. This can be done by listing a specific person, department, or job function. Authorization includes vendors and the entity's personnel. Caution: consider whether these user(s) must have authorized electronic access to the applicable system in accordance with CIP-004.
- Locations where the Removable Media may be used. This can be done by listing a specific location or a group/role of locations.

Section 3.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The entities must use the method(s) to detect malicious code on Removable Media before it is connected to the BES Cyber Asset. The timing dictated and documented in the entity's plan should reduce the risk of introducing malicious code to the BES Cyber Asset or Protected Cyber Asset.

For Section 3.2.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System or Protected Cyber Asset.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

Requirement R1 Part 1.6 addresses directives in Order No. 829 for verifying software integrity and authenticity prior to installation in BES Cyber Systems (P. 48). The objective of verifying software integrity and authenticity is to ensure that the software being installed in the BES Cyber System was not modified without the awareness of the software supplier and is not counterfeit.

Rationale for Requirement R2:

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

Rationale for Requirement R3:

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

Rationale for Requirement R4:

Requirement R4 responds to the directive in FERC Order No. 791, at Paragraphs 6 and 136, to address security-related issues associated with Transient Cyber Assets and Removable Media used on a temporary basis for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To mitigate the risks associated with such tools, Requirement R4 was developed to accomplish the following security objectives:

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.
- Requirement R4 incorporates the concepts from other CIP requirements in CIP-010-2 and CIP-007-6 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes:

All requirements related to Transient Cyber Assets and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT Implementation Guidance pending submittal for ERO Enterprise Endorsement

DRAFT

Cyber Security — Configuration Change Management and Vulnerability Assessments

Implementation Guidance for Reliability Standard CIP-010-4

October 2020

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

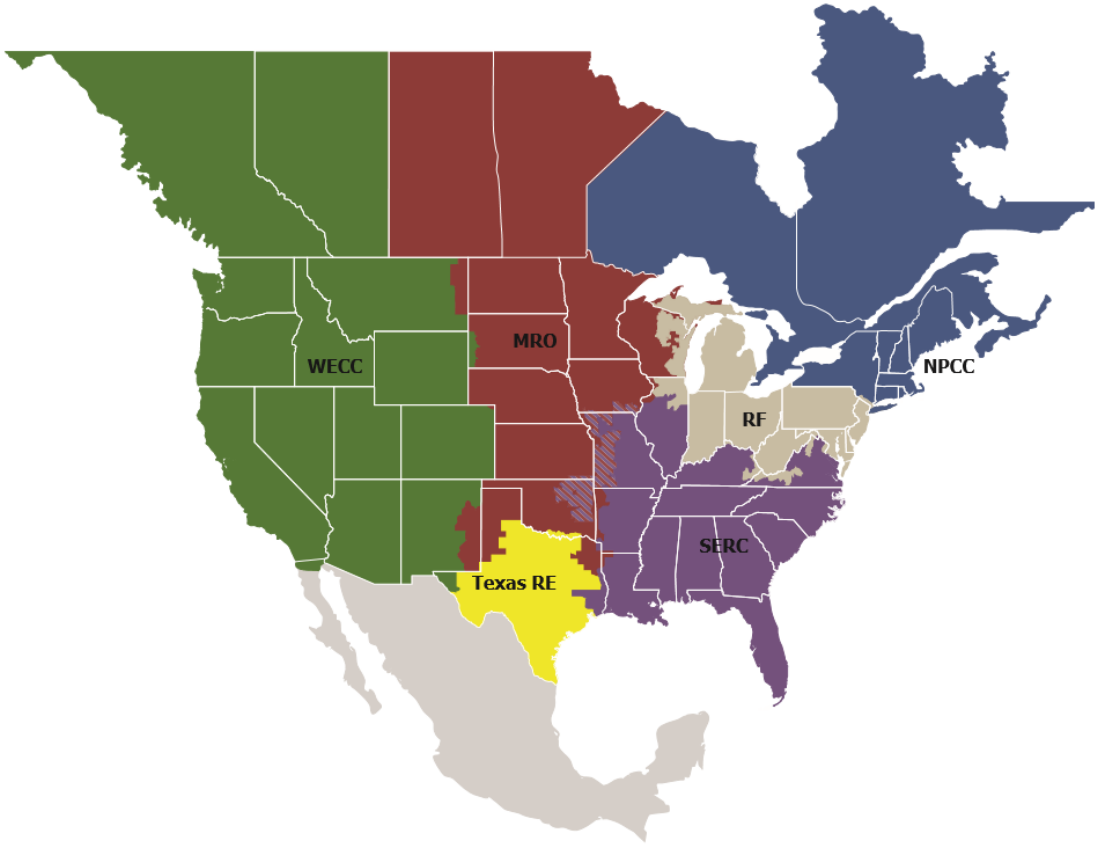
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

This Implementation Guidance was prepared to provide example approaches for compliance with CIP-010-4. Implementation Guidance does not prescribe the only approach but highlights one or more approaches that could be effective in achieving compliance with the standard. Because Implementation Guidance only provides one or more examples, entities may choose alternative approaches that better fit their individual situations.[1] This Implementation Guidance for CIP-010-4 is not a Reliability Standard and should not be considered mandatory and enforceable.

Responsible entities may find it useful to consider this Implementation Guidance document along with the additional context and background provided in the SDT-developed Technical Rationale and Justification for the modifications to CIP-010-4.

This document is composed of approaches written by previous drafting teams, relevant to previous versions of CIP-010, as well as additions by the Standards Project 2019-03 – Cyber Security Supply Chain Risks Standards Drafting Team (SDT) related to the modifications. Anything relevant to version 4 of this standard that was written by previous SDT's is included in this document.

Project 2019-03 was initiated due to the Federal Energy Regulatory Commission (the Commission) issuing Order No. 850[2] on October 18, 2018, in which the summary on page 1 states, "…the Comission directs NERC to develop and submit modifications to the supply chain risk management Reliability Standards so that the scope of the Reliability Standards include Electronic Access Control and Monitoring Systems." In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report, Staff Report and Recommended Actions[3], to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT modified Reliability Standard CIP-010-4 to require responsible entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

[1] NERC's Compliance Guidance Policy

[2] https://www.ferc.gov/whats-new/comm-meet/2018/101818/E-1.pdf

[3] https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

Requirement R1

General Considerations for Requirement R1

FERC Order 850, Paragraph 5 and Paragraph 30 directed modifications to Reliability Standard CIP-010-3 Requirement R1 to address supply chain risk management for Electronic Access Control or Monitoring Systems (EACMS) for high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards to address PACS that provide physical access control (excluding alarming and logging) to high and medium impact BES Cyber Systems, and modifications were addressed by the 2019-03 SDT.

General Considerations for Requirement R1 Part 1.5

Test Environment

The Responsible Entity should note that wherever a test environment (or the test is performed in production in a manner that minimizes adverse effects) is mentioned, entities are required to "model" the baseline configuration and not duplicate it exactly.

The language for use of a testing environment for deviations from baseline configuration was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

General Considerations for Requirement R1 Part 1.6

Software Verification

NIST SP-800-161 includes a number of security controls, which together reduce the probability of a successful "Watering Hole" or similar cyber-attack in the industrial control system environment and thus could assist in addressing this objective. For example, in the System and Information Integrity (SI) control family, control SI-7 suggests users obtain software directly from the developer and verify the integrity of the software using controls such as digital signatures. In the Configuration Management (CM) control family, control CM-5(3) requires information systems prevent the installation of firmware or software without digital signature verification so genuine and valid hardware and software components are used. NIST SP-800-161, while not meant to be definitive, provides examples of controls for addressing this objective. Other controls also could meet this objective.

In implementing Requirement R1 Part 1.6, the responsible entity should consider their existing CIP cyber security policies and controls in addition to the following:

- Processes used to deliver software and appropriate control(s) that will verify the identity of the software source and the integrity of the software delivered through these processes. To the extent that the responsible entity utilizes automated systems such as a subscription service to download and distribute software including updates, consider how software verification can be performed through those processes.
- Coordination of the responsible entity's software verification control(s) with other cyber security policies and controls, including change management and patching processes, and procurement controls.
- Use of a secure central software repository after the identity of the software source and the integrity of the software have been validated, so that verifications do not need to be performed repeatedly before each installation.
- Additional controls such as examples outlined in the Software, Firmware, and Information Integrity (SI-7) section of NIST Special Publication 800-53 Revision 4, or similar guidance.
- Additional controls such as those defined in FIPS-140-2, FIPS 180-4, or similar guidance, to ensure the cryptographic methods used are acceptable to the Responsible Entity.

Responsible entities may use various methods to verify the integrity of software obtained from the software source. Examples include, but are not limited to, the following:

- Verify and validate digital signature on the software to detect modifications indication compromise of the software's integrity.
- Use public key infrastructure (PKI) with encryption as a method to prevent software modification in transit by enabling only intended recipients to decrypt the software.
- Require fingerprints or cipher hashes from software sources for all software and compare the values to the authoritative source prior to installation on a BES Cyber System as verification of the integrity of the software. Consider using a method for receiving the verification values that is different from the method used to receive the software from the software source.
- Use trusted/controlled distribution and delivery options to reduce supply chain risk (e.g., requiring tamper-evident packaging of software during shipping.)

Even after verification is completed, it is still recommended that software testing is performed. If the integrity and authenticity checks are only performed at vendor point of origin, there is no guarantee that the product being retrieved is untainted prior to availability at the point of origin. The vendor checks performed do not detect embedded malicious code in the software, firmware or patch between the vendor applying the integrity method and the implementation of the software by the Registered Entity on a high or medium impact BES Cyber System and its associated EACMS or PACS.

Implementation Guidance for R1

Refer to ERO Enterprise Endorsed Implementation Guidance document CIP-010-3 R1.6 Software Integrity and Authenticity for additional compliance guidance and examples etc.

Implementation Guidance for CIP-010-3

This section contains a "cut and paste" of the Implementation Guidance components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-010-3 standard to preserve any historical references. Similarly, former GTB content providing SDT intent and technical rationale can be found in a separate Technical Rational document for this standard.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards:

None

Requirement R1:

Baseline Configuration

Further guidance can be understood with the following example that details the baseline configuration for a serial-only microprocessor relay:

Asset #051028 at Substation Alpha

- R1.1.1 – Firmware: [MANUFACTURER]-[MODEL]-XYZ-1234567890-ABC
- R1.1.2 – Not Applicable
- R1.1.3 – Not Applicable
- R1.1.4 – Not Applicable
- R1.1.5 – Patch 12345, Patch 67890, Patch 34567, Patch 437823

Also, for a typical IT system, the baseline configuration could reference an IT standard that includes configuration details. An entity would be expected to provide that IT standard as part of their compliance evidence.

Cyber Security Controls

None

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components. For instance, an entity may have a BES Cyber System that runs a database on one component and a web server on another component. The test environment may have the same operating system, security patches, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple components.

This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

Software Verification

NIST SP-800-161 includes a number of security controls, which, when taken together, reduce the probability of a successful "Watering Hole" or similar cyber attack in the industrial control system environment and thus could assist in addressing this objective. For example, in the System and Information Integrity (SI) control family, control SI-7 suggests users obtain software directly from the developer and verify the integrity of the software using controls such as digital signatures. In the Configuration Management (CM) control family, control CM-5(3) requires that the

information system prevent the installation of firmware or software without the verification that the component has been digitally signed to ensure that the hardware and software components are genuine and valid. NIST SP-800-161, while not meant to be definitive, provides examples of controls for addressing this objective. Other controls also could meet this objective.

In implementing Requirement R1 Part 1.6, the responsible entity should consider their existing CIP cyber security policies and controls in addition to the following:

- Processes used to deliver software and appropriate control(s) that will verify the identity of the software source and the integrity of the software delivered through these processes. To the extent that the responsible entity utilizes automated systems such as a subscription service to download and distribute software including updates, consider how software verification can be performed through those processes.
- Coordination of the responsible entity's software verification control(s) with other cyber security policies and controls, including change management and patching processes, and procurement controls.
- Use of a secure central software repository after the identity of the software source and the integrity of the software have been validated, so that verifications do not need to be performed repeatedly before each installation.
- Additional controls such as examples outlined in the Software, Firmware, and Information Integrity (SI-7) section of NIST Special Publication 800-53 Revision 4, or similar guidance.
- Additional controls such as those defined in FIPS-140-2, FIPS 180-4, or similar guidance, to ensure the cryptographic methods used are acceptable to the Responsible Entity.

Responsible entities may use various methods to verify the integrity of software obtained from the software source. Examples include, but are not limited to, the following:

- Verify that the software has been digitally signed and validate the signature to ensure that the software's integrity has not been compromised.
- Use public key infrastructure (PKI) with encryption to ensure that the software is not modified in transit by enabling only intended recipients to decrypt the software.
- Require software sources to provide fingerprints or cipher hashes for all software and verify the values prior to installation on a BES Cyber System to ensure the integrity of the software. Consider using a method for receiving the verification values that is different from the method used to receive the software from the software source.
- Use trusted/controlled distribution and delivery options to reduce supply chain risk (e.g., requiring tamper-evident packaging of software during shipping.)

Requirement R2:

However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

In developing their vulnerability assessment processes, Responsible Entities are strongly encouraged to include at least the following elements, several of which are referenced in CIP-005 and CIP-007:

Paper Vulnerability Assessment:

1. Network Discovery - A review of network connectivity to identify all Electronic Access Points to the Electronic Security Perimeter.
2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification.
3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings.
4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications.

Active Vulnerability Assessment:

1. Network Discovery - Use of active discovery tools to discover active devices and identify communication paths in order to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification – Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning – Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning – Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within the range of the wireless scanning tool.

In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.

Requirement R4:

Examples of these temporarily connected devices include, but are not limited to:

- Diagnostic test equipment;
- Packet sniffers;
- Equipment used for BES Cyber System maintenance;
- Equipment used for BES Cyber System configuration; or
- Equipment used to perform vulnerability assessments.

The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset, BES Cyber Asset, or Protected Cyber Asset.

<u>Per Transient Cyber Asset Capability</u>

For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.2: To meet this requirement part, the entity is to document the following:

1.2.1 User(s), individually or by group/role, allowed to use the Transient Cyber Asset(s). This can be done by listing a specific person, department, or job function. Caution: consider whether these user(s) must also have authorized electronic access to the applicable system in accordance with CIP-004.

1.2.2 Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group of locations.

1.2.3 The intended or approved use of each individual, type, or group of Transient Cyber Asset. This should also include the software or application packages that are authorized with the purpose of performing defined business functions or tasks (e.g., used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes), and approved network interfaces (e.g., wireless, including near field communication or Bluetooth, and wired connections). Activities, and software or application packages, not specifically listed as acceptable should be considered as prohibited. It may be beneficial to educate individuals through the CIP-004 Security Awareness Program and Cyber Security Training Program about authorized and unauthorized activities or uses (e.g., using the device to browse the Internet or to check email or using the device to access wireless networks in hotels or retail locations).

Entities should exercise caution when using Transient Cyber Assets and ensure they do not have features enabled (e.g., wireless or Bluetooth features) in a manner that would allow the device to bridge an outside network to an applicable system. Doing so would cause the Transient Cyber Asset to become an unauthorized Electronic Access Point in violation of CIP-005, Requirement R1.

Attention should be paid to Transient Cyber Assets that may be used for assets in differing impact areas (i.e., high impact, medium impact, and low impact). These impact areas have differing levels of protection under the CIP requirements, and measures should be taken to prevent the introduction of malicious code from a lower impact area. An entity may want to consider the need to have separate Transient Cyber Assets for each impact level.

Section 1.3: Options are listed that include the alternative for the entity to use a technology or process that effectively mitigates vulnerabilities.

- Security patching, including manual or managed updates provides flexibility to the Responsible Entity to determine how its Transient Cyber Asset(s) will be used. It is possible for an entity to have its Transient Cyber Asset be part of an enterprise patch process and receive security patches on a regular schedule or the entity can verify and apply security patches prior to connecting the Transient Cyber Asset to an applicable Cyber Asset. Unlike CIP-007, Requirement R2, there is no expectation of creating dated mitigation plans or other documentation other than what is necessary to identify that the Transient Cyber Asset is receiving appropriate security patches.
- Live operating system and software executable only from read-only media is provided to allow a protected operating system that cannot be modified to deliver malicious software. When entities are creating custom live operating systems, they should check the image during the build to ensure that there is not malicious software on the image.
- System hardening, also called operating system hardening, helps minimize security vulnerabilities by removing all non-essential software programs and utilities and only installing the bare necessities that the computer needs to function. While other programs may provide useful features, they can provide "back-door" access to the system, and should be removed to harden the system.

- When selecting to use other methods that mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet the software vulnerability mitigation objective.

Section 1.4: Entities should also consider whether the detected malicious code is a Cyber Security Incident.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility just as with security patching, to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the opportunity that malicious software could become resident, much less propagate, from the Transient Cyber Asset to the BES Cyber Asset or BES Cyber System.
- Restricted communication to limit the exchange of data to only the Transient Cyber Asset and the Cyber Assets to which it is connected by restricting or disabling serial or network (including wireless) communications on a managed Transient Cyber Asset can be used to minimize the opportunity to introduce malicious code onto the Transient Cyber Asset while it is not connected to BES Cyber Systems. This renders the device unable to communicate with devices other than the one to which it is connected.
- When selecting to use other methods that mitigate the introduction of malicious code to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the introduction of malicious code objective.

Section 1.5: The bulleted list of example protections provides some suggested alternatives.

- For restricted physical access, the intent is that the Transient Cyber Asset is maintained within a Physical Security Perimeter or other physical location or enclosure that uses physical access controls to protect the Transient Cyber Asset.
- Full disk encryption with authentication is an option that can be employed to protect a Transient Cyber Asset from unauthorized use. However, it is important that authentication be required to decrypt the device. For example, pre-boot authentication, or power-on authentication, provides a secure, tamper-proof environment external to the operating system as a trusted authentication layer. Authentication prevents data from being read from the hard disk until the user has confirmed they have the correct password or other credentials. By performing the authentication prior to the system decrypting and booting, the risk that an unauthorized person may manipulate the Transient Cyber Asset is mitigated.
- Multi-factor authentication is used to ensure the identity of the person accessing the device. Multi-factor authentication also mitigates the risk that an unauthorized person may manipulate the Transient Cyber Asset.
- In addition to authentication and pure physical security methods, other alternatives are available that an entity may choose to employ. Certain theft recovery solutions can be used to locate the Transient Cyber Asset, detect access, remotely wipe, and lockout the system, thereby mitigating the potential threat from unauthorized use if the Transient Cyber Asset was later connected to a BES Cyber Asset. Other low tech solutions may also be effective to mitigate the risk of using a maliciously-manipulated Transient Cyber Asset, such as tamper evident tags or seals, and executing procedural controls to verify the integrity of the tamper evident tag or seal prior to use.

- When selecting to use other methods that mitigate the risk of unauthorized use to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the risk of unauthorized use objective.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

To facilitate these controls, Responsible Entities may choose to execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014[4]. Procurement language may unify the other party and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the other party's support. Entities should consider the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.

Section 2.1: Entities are to document and implement their process(es) to mitigate software vulnerabilities through the use of one or more of the protective measures listed.

- Conduct a review of the Transient Cyber Asset managed by a party other than the Responsible Entity to determine whether the security patch level of the device is adequate to mitigate the risk of software vulnerabilities before connecting the Transient Cyber Asset to an applicable system.
- Conduct a review of the other party's security patching process. This can be done either at the time of contracting but no later than prior to connecting the Transient Cyber Asset to an applicable system. Just as with reviewing the security patch level of the device, selecting to use this approach aims to ensure that the Responsible Entity has mitigated the risk of software vulnerabilities to applicable systems.
- Conduct a review of other processes that the other party uses to mitigate the risk of software vulnerabilities. This can be reviewing system hardening, application whitelisting, virtual machines, etc.
- When selecting to use other methods to mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet mitigation of the risk of software vulnerabilities.

Section 2.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.

[4] http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014

- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This will limit the chance of introducing malicious software to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

Section 3.1: Entities are to document and implement their process(es) to authorize the use of Removable Media. The Removable Media may be listed individually or by type.

- Document the user(s), individually or by group/role, allowed to use the Removable Media. This can be done by listing a specific person, department, or job function. Authorization includes vendors and the entity's personnel. Caution: consider whether these user(s) must have authorized electronic access to the applicable system in accordance with CIP-004.
- Locations where the Removable Media may be used. This can be done by listing a specific location or a group/role of locations.

Entities should also consider whether the detected malicious code is a Cyber Security Incident.

As a method to detect malicious code, entities may choose to use Removable Media with on-board malicious code detection tools. For these tools, the Removable Media are still used in conjunction with a Cyber Asset to perform the detection

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT

Cyber Security — Supply Chain Risk Management

Technical Rationale and Justification for Reliability Standard CIP-013-2

October 2020

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

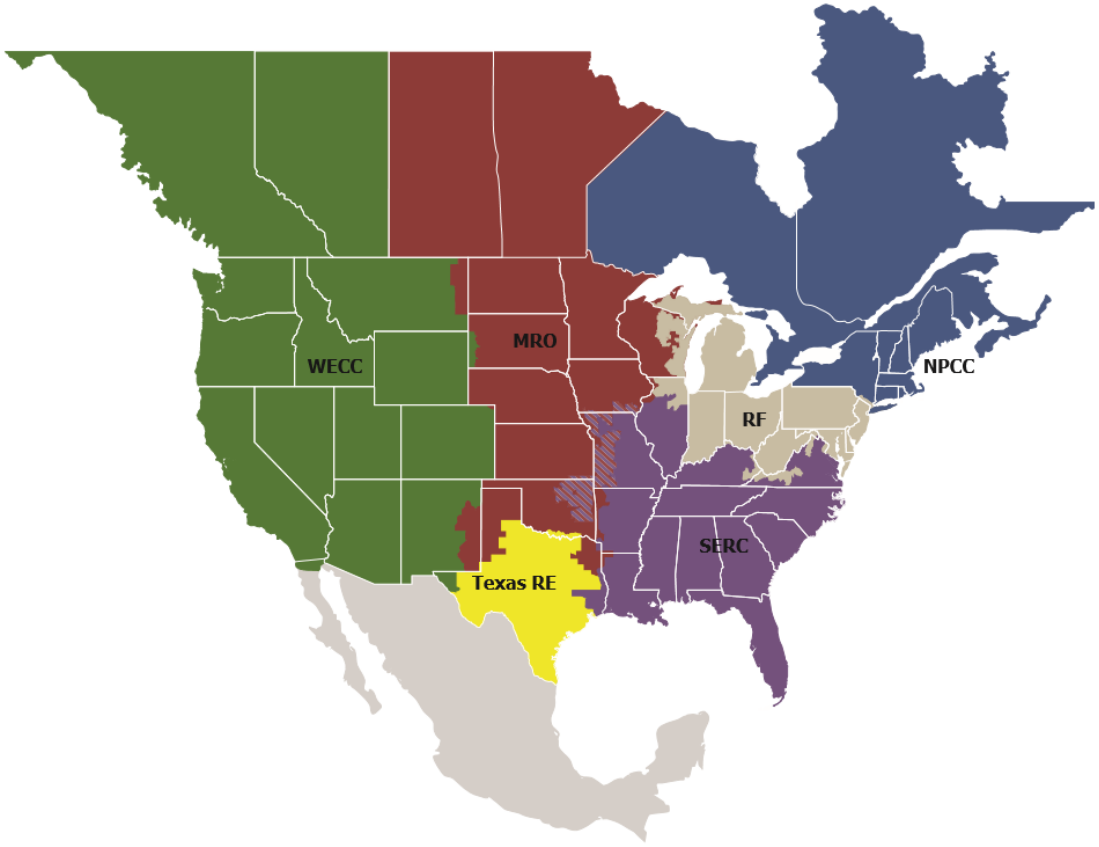
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-013-2. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. It also contains information on Project 2019-03 Cyber Security Supply Chain Risks Standard Drafting Team's (SDT's) intent in drafting the requirements. This Technical Rationale and Justification for CIP-013-2 is not a Reliability Standard and should not be considered mandatory and enforceable.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 850 on October 18, 2018, calling for modifications to the Supply Chain Suite of Standards to address Electronic Access Control or Monitoring Systems (EACMS), specifically those systems that provide electronic access control or monitoring to high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT drafted Reliability Standard CIP-013-2 to require responsible entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

New and Modified Terms Used on NERC Reliability Standards

CIP-013-2 uses the following definition(s), which are cited below for reference when reading the technical rationale that follows.

Proposed Modified Terms: None

Proposed New Terms: None

Requirement R1 and R2

General Considerations for Requirements R1 and R2

The Requirement addresses Order No. 829 directives for entities to develop and implement a plan(s) that includes processes for mitigating cyber security risks in the supply chain. The plan(s) is required to address the following four objectives (Order No. 829 at P. 45):

(1) Software integrity and authenticity;

(2) Vendor remote access;

(3) Information system planning; and

(4) Vendor risk management and procurement controls.

The cyber security risk management plan(s) specified in Requirement R1 apply to high and medium impact BES Cyber Systems. FERC Order 850, Paragraph 5 and Paragraph 30, directs modifications to Reliability Standards to include EACMS associated with medium and high impact BES Cyber Systems within the scope of the Supply Chain Risk Management Standards. In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report [1](Chapter 3, pages 12-15) to address PACS that provide physical access control to high and medium impact BES Cyber Systems.

Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders), consistent with Order No. 829 (P. 36).

Due to the nature of PACS and the potential need for physical presence, the SDT conducted extensive dialogue and consideration for the addition of PACS to the requirements. The SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warrants the inclusion of PACS as an applicable Cyber Asset category for supply chain risk management controls.

Further, the inclusion of PACS:

1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",
2. addresses the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and
3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "*Cyber Security Supply Chain Risks*"[2].

In further support of the SDT's decision to include PACS, as cited on page 4 of NERC's final report on "*Cyber Security Supply Chain Risks*", "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." While this statement appears in the context of EACMS, it acknowledges physical security threats equally; therefore, the concept is transferable and applicable to PACS, which serve as an integral component to a strategy involving layers of detective and preventive security controls. PACS are intended to manage physical access to BES Cyber Systems in support of protecting BES Cyber Systems against

[1] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

[2] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

compromise that could lead to misoperation or instability in the BES and are implemented with that specific intention to protect the BES Cyber System.

Additionally, NERC states on page 15 of their final report on "*Cyber Security Supply Chain Risks"* that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical access or monitoring controls that have not been compromised in order to gain access." While a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it could demonstrate a threat Actor's intention to gain fully unauthorized electronic access. With electronic access to the PACS an initial deliberate action to facilitate reconnaissance and intentional harm to the BES Cyber Systems.

Furthermore, there is precedent set in CIP-006-6 Requirement R1 Part 1.5 that speaks to a recognized importance of PACS, its functions, and the timeliness of information provided by these systems by requiring issuance of an alarm or alert in response to detected unauthorized access through a physical access point into a PSP to incident response personnel within 15 minutes of detection. This strict timeline suggests imminent threat that compromised physical security poses to the associated BES Cyber System and the reliable operation of the BES Facilities it serves.

The SDT agrees that NERC correctly refers to various Reliability Standards that mitigate certain security risks relating to PACS; however, the SDT asserts that these existing requirements do not address risk associated to the supply chain and therefore do not sufficiently mitigate that risk.

An additional aspect of the NERC Supply Chain Report the SDT considered was around the risk associated with the different aspects of both EACMS and PACS. While both types of systems, under the current definitions, have various functional activities they perform, the NERC Supply Chain Report pointed to the increased risk of the control function. The SDT considered limiting the scope of the requirements to only control functions, however chose to stay with the currently approved definitions of both EACMS and PACS. The SDT concluded staying with approved definitions would introduce less confusion. Additionally an attempt to change the EACMS and PACS definitions was outside the 2019-03 SAR.

Rational for Requirement 1 and Requirement 2

Requirement R1 Part 1.1 addresses the directive in Order No. 829 (P.56) and Order 850 (P.5) for identification and documentation of cyber security risks in the planning and development processes related to the procurement of medium and high impact BES Cyber Systems, and their associated EACMS and PACS. The security objective is to ensure entities consider cyber security risks to the BES from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s); and options for mitigating these risks when planning for BES Cyber Systems.

Requirement R1 Part 1.2 addresses the directive in Order No. 829 for procurement controls to address the provision and verification of security concepts in future contracts for BES Cyber Systems (P. 59). The objective of Part 1.2 is for entities to include these topics in their plans so that procurement and contract negotiation processes address the applicable risks. Implementation of the entity's plan related to Part 1.2 may be accomplished through the entity's procurement and contract negotiation processes. For example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs), negotiations with vendors, or requests submitted to entities negotiating on behalf of the Responsible Entity such as in cooperative purchasing agreements. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan. Although the expectation is that Responsible Entities would enforce the security-related provisions in the contract based on the terms and conditions of that contract, such contract enforcement and vendor performance or adherence to the negotiated contract is not subject to this Reliability Standard.

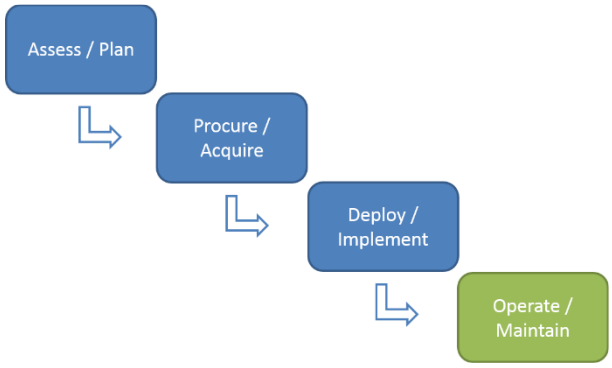
The objective of verifying software integrity and authenticity (Part 1.2.5) is to help ensure that software installed on BES Cyber Systems is not modified prior to installation without the awareness of the software supplier and is not counterfeit. Part 1.2.5 is not an operational requirement for entities to perform such verification; instead, it requires entities to address the software integrity and authenticity issue in its contracting process to provide the entity the means by which to perform such verification under CIP-010-3.

The use of remote access in Part 1.2.6 includes vendor-initiated authenticated remote connections and system to system remote connections for EACMS and PACS; and vendor-initiated IRA and system to system access to BCS and PCAs.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Collectively, the provisions of CIP-013-2 address an entity's controls for managing cyber security risks to BES Cyber Systems during the planning, acquisition, and deployment phases of the system life cycle, as shown below.

Notional BES Cyber System Life Cycle



Requirement R3

General Considerations for Requirement R3

The requirement addresses Order No. 829 directives for entities periodically to reassess selected supply chain cyber security risk management controls (P. 46).

Entities perform periodic assessment to keep plans up-to-date and address current and emerging supply chain-related concerns and vulnerabilities. Examples of sources of information that the entity could consider include guidance or information issued by:

- NERC or the E-ISAC
- ICS-CERT
- Canadian Cyber Incident Response Centre (CCIRC)

Responsible Entities are not required to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders) when implementing an updated plan (i.e., the note in Requirement R2 applies to implementation of new plans and updated plans).

Technical Rational for Reliability Standard CIP-013-1

This section contains a "cut and paste" of the Technical Rationale components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-013-1 standard to preserve any historical references. Similarly, former GTB content providing compliance guidance can be found in a separate Implementation Guidance document for this standard.

Rationale

Requirement R1:

The proposed Requirement addresses Order No. 829 directives for entities to implement a plan(s) that includes processes for mitigating cyber security risks in the supply chain. The plan(s) is required to address the following four objectives (Order No. 829 at P. 45):

(1) Software integrity and authenticity;

(2) Vendor remote access;

(3) Information system planning; and

(4) Vendor risk management and procurement controls.

The cyber security risk management plan(s) specified in Requirement R1 apply to high and medium impact BES Cyber Systems.

Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders), consistent with Order No. 829 (P. 36).

Requirement R1 Part 1.1 addresses the directive in Order No. 829 for identification and documentation of cyber security risks in the planning and development processes related to the procurement of BES Cyber Systems (P. 56). The security objective is to ensure entities consider cyber security risks to the BES from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s); and options for mitigating these risks when planning for BES Cyber Systems.

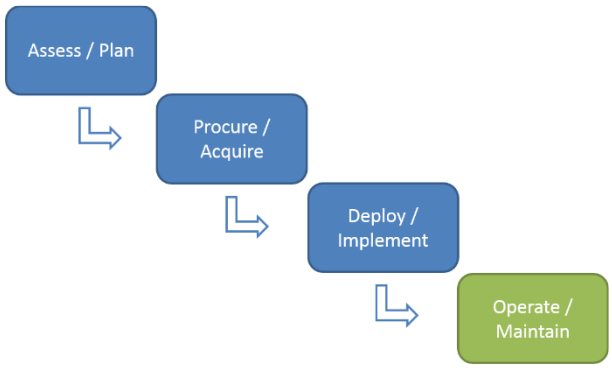
Requirement R1 Part 1.2 addresses the directive in Order No. 829 for procurement controls to address the provision and verification of security concepts in future contracts for BES Cyber Systems (P. 59). The objective of Part 1.2 is for entities to include these topics in their plans so that procurement and contract negotiation processes address the applicable risks. Implementation of the entity's plan related to Part 1.2 may be accomplished through the entity's procurement and contract negotiation processes. For example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs), negotiations with vendors, or requests submitted to entities negotiating on behalf of the Responsible Entity such as in cooperative purchasing agreements. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan. Although the expectation is that Responsible Entities would enforce the security-related provisions in the contract based on the terms and conditions of that contract, such contract enforcement and vendor performance or adherence to the negotiated contract is not subject to this Reliability Standard.

The objective of verifying software integrity and authenticity (Part 1.2.5) is to help ensure that software installed on BES Cyber Systems is not modified prior to installation without the awareness of the software supplier and is not counterfeit. Part 1.2.5 is not an operational requirement for entities to perform such verification; instead, it requires entities to address the software integrity and authenticity issue in its contracting process to provide the entity the means by which to perform such verification under CIP-010-3.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Collectively, the provisions of CIP-013-1 address an entity's controls for managing cyber security risks to BES Cyber Systems during the planning, acquisition, and deployment phases of the system life cycle, as shown below.

Notional BES Cyber System Life Cycle



Requirement R2:

The proposed requirement addresses Order No. 829 directives for entities to periodically reassess selected supply chain cyber security risk management controls (P. 46).

Entities perform periodic assessment to keep plans up-to-date and address current and emerging supply chain-related concerns and vulnerabilities. Examples of sources of information that the entity could consider include guidance or information issued by:

- NERC or the E-ISAC
- ICS-CERT
- Canadian Cyber Incident Response Centre (CCIRC)

Responsible Entities are not required to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders) when implementing an updated plan (i.e., the note in Requirement R2 applies to implementation of new plans and updated plans).

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT

Cyber Security Supply Chain Risk Management Plans

Implementation Guidance for Reliability Standard CIP-013-2

October 2020

RELIABILITY | ACCOUNTABILITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

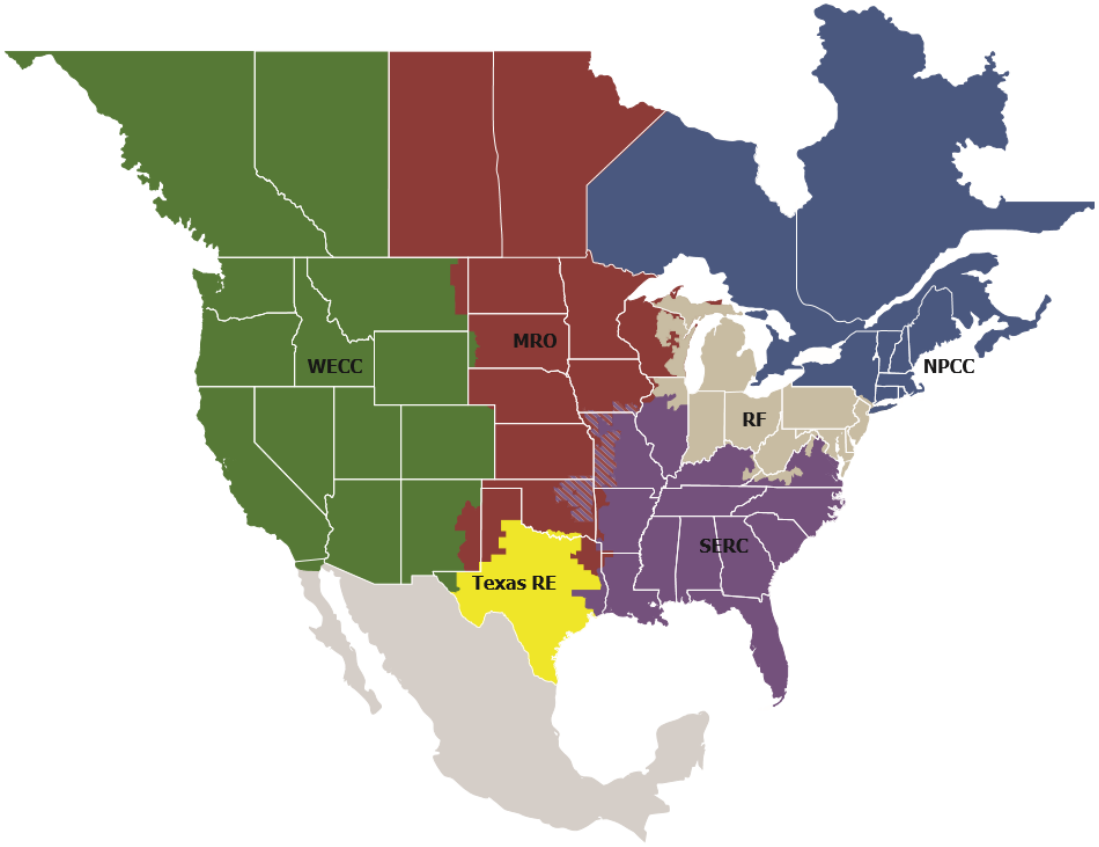
Table of Contents

Preface

*Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. T*he vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

On July 21, 2016, the Federal Energy Regulatory Commission (FERC) issued Order No. 829 directing the North American Electric Reliability Corporation (NERC) to develop a new or modified Reliability Standard that addresses cyber security supply chain risk management for industrial control system hardware, software, and computing and networking services associated with Bulk Electric System (BES) operations as follows:

> [The Commission directs] NERC to develop a forward-looking, objective-based Reliability Standard to require each affected entity to develop and implement a plan that includes security controls for supply chain management for industrial control system hardware, software, and services associated with bulk electric system operations. The new or modified Reliability Standard should address the following security objectives, [discussed in detail in the Order]: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls.

On October 18, 2018, the Federal Energy Regulatory Commission (FERC) issued Order No. 850 approving the supply chain risk management Reliability Standards CIP-013-1 (Cyber Security – Supply Chain Risk Management), CIP-005-6 (Cyber Security – Electronic Security Perimeter(s) and CIP-010-3 (Cyber Security – Configuration Change Management and Vulnerability Assessments) submitted by the North American Electric Reliability Corporation (NERC), and directing NERC to include Electronic Access Control or Monitoring Systems (EACMS).

On May 17, 2019, NERC published Cyber Security Supply Chain Risks Report recommending the inclusion of Physical Access Control Systems (PACS).

Reliability Standard **CIP-013-2 – Cyber Security – Supply Chain Risk Management** addresses the relevant cyber security supply chain risks in the planning, acquisition, and deployment phases of the system life cycle for high and medium impact BES Cyber Systems[1] and their associated EACMS and PACS.

This implementation guidance provides considerations for implementing the requirements in CIP-013-2 and examples of approaches that responsible entities could use to meet the requirements. The examples do not constitute the only approach to complying with CIP-013-2. Responsible Entities may choose alternative approaches that better fit their situation.

[1] Responsible Entities identify high and medium impact BES Cyber Systems, and their associated EACMS and PACS, according to the identification and categorization process required by CIP-002-5, or subsequent version of that standard.

Requirement R1

R1. *Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems and their associated EACMS and PACS. The plan(s) shall include:*

1.1. *One or more process(es) used in planning for the procurement of BES Cyber Systems and their associated EACMS and PACS to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).*

1.2. *One or more process(es) used in procuring BES Cyber Systems, and their associated EACMS and PACS, that address the following, as applicable:*

1.2.1. *Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;*

1.2.2. *Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;*

1.2.3. *Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;*

1.2.4. *Disclosure by vendors of known vulnerabilities;*

1.2.5. *Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System; and*

1.2.6. *Coordination of controls for vendor-initiated remote access.*

General Considerations for R1

The following are some general considerations for Responsible Entities as they implement Requirement R1:

First, in developing their supply chain cyber security risk management plan(s), Responsible entities should consider how to leverage the various components and phases of their processes (e.g. defined requirements, request for proposal, bid evaluation, external vendor assessment tools and data, third party certifications and audit reports, etc.) to help them meet the objective of Requirement R1 and give them flexibility to negotiate contracts with vendors to efficiently mitigate risks. Focusing solely on the negotiation of specific contract terms could have unintended consequences, including significant and unexpected cost increases for the product or service or vendors refusing to enter into contracts.

Additionally, a Responsible Entity may not have the ability to obtain each of its desired cyber security controls in its contract with each of its vendors. Factors such as competition, limited supply sources, expense, criticality of the product or service, and maturity of the vendor or product line could affect the terms and conditions ultimately negotiated by the parties and included in a contract. This variation in contract terms is anticipated and, in turn, the note in Requirement R2 provides that the actual terms and conditions of the contract are outside the scope of Reliability Standard CIP-013-2.

> *Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.*

The focus of Requirement R1 is on the steps the Responsibility Entity takes to consider cyber security risks from vendor products or services during BES Cyber System planning and procurement. In the event the vendor is unwilling to engage in the negotiation process for cyber security controls, the Responsible Entity could explore other sources of supply or mitigating controls to reduce the risk to the BES cyber systems, as the Responsible Entity's circumstances allow.

In developing and implementing its supply chain cyber security risk management plan, a Responsible Entity may consider identifying and prioritizing security controls based on the cyber security risks presented by the vendor and the criticality of the product or service to reliable operations. For instance, Responsible Entities may establish a baseline set of controls for given products or services that a vendor must meet prior to transacting with that vendor for those products and services (i.e., "must-have controls"). As risks differ between products and services, the baseline security controls – or "must haves" – may differ for the various products and services the Responsible Entities procures for its BES Cyber Systems. This risk-based approach could help create efficiencies in the Responsible Entity's procurement processes while meeting the security objectives of Requirement R1.

The objective of addressing the verification of software integrity and authenticity during the procurement phase of BES Cyber System(s) (Part 1.2.5) is to identify the capability of the vendor(s) to ensure that the software installed on BES Cyber System(s) is trustworthy. Part 1.2.5 is not an operational requirement for Responsible Entities to perform the verification; instead, Part 1.2.5 is aimed at identifying during the procurement phase the vendor's capability to provide software integrity and authenticity assurance and establish vendor performance based on the vendor's capability in order to implement CIP-010-4, Requirement R1, Part 1.6.

Implementation Guidance for R1

Responsible entities use various processes as they plan to procure BES Cyber Systems. Below are some examples of approaches to comply with this requirement:

R1. *Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems and their associated EACMS and PACS. The plan(s) shall include:*

- The Responsible Entity could establish one or more documents explaining the process by which the Responsible Entity will address supply chain cyber security risk management for high and medium impact BES Cyber Systems and their associated EACMS and PACS. To achieve the flexibility needed for supply chain cyber security risk management, Responsible Entities can use a "risk-based approach". One element of, or approach to, a risk-based cyber security risk management plan is **system-based**, focusing on specific controls for high and medium impact BES Cyber Systems and their associated EACMS and PACS to address the risks presented in procuring those systems or services for those systems. A risk-based approach could also be **vendor-based**, focusing on the risks posed by various vendors of its BES Cyber Systems. Entities may combine both of these approaches into their plans. This flexibility is important to account for the varying "needs and characteristics of responsible entities and the diversity of BES Cyber System environments, technologies, and risk (FERC Order No. 829 P 44)."

  1.1. *One or more process(es) used in planning for the procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).*

A Responsible Entity could document in its supply chain cyber security risk management plan one or more processes that it will use when planning for the procurement of BES Cyber Systems to identify and assess cyber security risks to the Bulk Electric System from vendor products or services as specified in the requirement. Examples of processes, or outcomes of these processes, for complying with Part 1.1 are described below. A Responsible Entity could comply with Part 1.1 using either the first (team review)

approach, or the second (risk assessment process) approach, a combination of the two approaches, or another approach determined by the Responsible Entity to comply with Part 1.1.

- A Responsible Entity can develop a process to form a team of subject matter experts from across the organization to participate in the BES Cyber System planning and acquisition process(es). The Responsible Entity should consider the relevant subject matter expertise necessary to meet the objective of Part 1.1 and include the appropriate representation of business operations, security architecture, information communications and technology, supply chain, compliance, and legal. Examples of factors that this team could consider in planning for the procurement of BES Cyber Systems as specified in Part 1.1 include:
  - Cyber security risk(s) to the BES that could be introduced by a vendor in new or planned modifications to BES Cyber Systems.
  - Vendor security processes and related procedures, including: system architecture, change control processes, remote access requirements, and security notification processes.
  - Periodic review processes that can be used with critical vendor(s) to review and assess any changes in vendor's security controls, product lifecycle management, supply chain, and roadmap to identify opportunities for continuous improvement.
  - Vendor use of third party (e.g., product/personnel certification processes) or independent review methods to verify product and/or service security practices.
  - Third-party security assessments or penetration testing provided by the vendors.
  - Vendor supply chain channels and plans to mitigate potential risks or disruptions.
  - Known system vulnerabilities; known threat techniques, tactics, and procedures; and related mitigation measures that could be introduced by vendor's information systems, components, or information system services.
  - Corporate governance and approval processes.
  - Methods to minimize network exposure, e.g., prevent internet accessibility, use of firewalls, and use of secure remote access techniques.
  - Methods to limit and/or control remote access from vendors to Responsible Entity's BES Cyber Systems.
  - Vendor's risk assessments and mitigation measures for cyber security during the planning and procurement process.
  - Mitigating controls that can be implemented by the Responsible Entity of the vendor. Examples include hardening the information system, minimizing the attack surface, ensuring ongoing support for system components, identification of alternate sources for critical components, etc.
- A Responsible Entity can develop a risk assessment process to identify and assess potential cyber security risks resulting from (i) procuring and installing vendor equipment and software and (ii) transitions from one vendor(s) to another vendor(s). This process could consider the following:
  - Potential risks based on the vendor's information systems, system components, and/or information system services / integrators. Examples of considerations include:
    - Critical systems, components, or services that impact the operations or reliability of BES Cyber Systems.
    - Product components that are not owned and managed by the vendor that may introduce additional risks, such as open source code or components from third party developers and manufacturers.

- Potential risks based on the vendor's risk management controls. Examples of vendor risk management controls to consider include[2]:
  - Personnel background and screening practices by vendors.
  - Training programs and assessments of vendor personnel on cyber security.
  - Formal vendor security programs which include their technical, organizational, and security management practices.
  - Vendor's physical and cyber security access controls to protect the facilities and product lifecycle.
  - Vendor's security engineering principles in (i) developing layered protections; (ii) establishing sound security policy, architecture, and controls as the foundation for design; (iii) incorporating security requirements into the system development lifecycle; (iv) delineating physical and logical security boundaries; (v) ensuring that system developers are training on how to build security software; (vi) tailoring security controls to meet organizational and operational needs; (vii) performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk; and (viii) reducing risk to acceptable levels, thus enabling informed risk management decisions. (NIST SP 800-53 SA-8 – Security Engineering Principles).
  - System Development Life Cycle program (SDLC) methodology from design through patch management to understand how cyber security is incorporated throughout the vendor's processes.
  - Vendor certifications and their alignment with recognized industry and regulatory controls.
  - Summary of any internal or independent cyber security testing performed on the vendor products to ensure secure and reliable operations.[3]
  - Vendor product roadmap describing vendor support of software patches, firmware updates, replacement parts and ongoing maintenance support.
  - Identify processes and controls for ongoing management of Responsible Entity and vendor's intellectual property ownership and responsibilities, if applicable. Examples include use of encryption algorithms for securing software code, data and information, designs, and proprietary processes while at rest or in transit.
- Based on risk assessment, identify mitigating controls that can be implemented by the Responsible Entity or the vendor. Examples include hardening the information system, minimizing the attack surface, ensuring ongoing support for system components, identification of alternate sources for critical components, etc.

1.2. *One or more process(es) used in procuring BES Cyber Systems that address the following, as applicable:*

[2] Tools such as the Standardized Information Gathering (SIG) Questionnaire from the Shared Assessments Program can aid in assessing vendor risk.

[3] For example, a Responsible Entity can request that the vendor provide a Standards for Attestation Engagements (SSAE) No. 18 SOC 2 audit report.

A Responsible Entity could document in its supply chain cyber security risk management plan one or more processes that it will use when procuring BES Cyber Systems to address Parts 1.2.1 through 1.2.6. The following are examples of processes, or outcomes of these processes, for complying with Part 1.2.

- Request cyber security terms relevant to applicable Parts 1.2.1 through 1.2.6 in the procurement process (request for proposal (RFP) or contract negotiation) for BES Cyber Systems to ensure that vendors understand the cyber security expectations for implementing proper security controls throughout the design, development, testing, manufacturing, delivery, installation, support, and disposition of the product lifecycle[4].
- During negotiations of procurement contracts or processes with vendors, the Responsible Entity can document the rationale, mitigating controls, or acceptance of deviations from the Responsible Entity's standard cyber security procurement language that is applicable to the vendor's system component, system integrators, or external service providers.

Examples of ways that a Responsible Entity could, through process(es) for procuring BES Cyber Systems required by Part 1.2, comply with Parts 1.2.1 through 1.2.6 are described below.

1.2.1. *Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;*

- In an RFP or during contract negotiations, request that the vendor include in the contract provisions an obligation for the vendor to provide notification of any identified, threatened, attempted or successful breach of vendor's components, software or systems (*e.g.,* "security event") that have potential adverse impacts to the availability or reliability of BES Cyber Systems. Security event notifications to the Responsible Entity should be sent to designated point of contact as determined by the Responsible Entity and vendor. Examples of information to request that vendor's include in notifications to the Responsible Entity are(i) mitigating controls that the Responsible Entity can implement, if applicable (ii) availability of patch or corrective components, if applicable.

1.2.2. *Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;*

- A Responsible Entity and vendor can agree on service level agreements for response to cyber security incidents and commitment from vendor to collaborate with the Responsible Entity in implement mitigating controls and product corrections.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor such that, in the event the vendor identifies a vulnerability that has resulted in a cyber security incident related to the products or services provided to the Responsible Entity, the vendor should provide notification to Responsible Entity. The contract could specify that the vendor provide defined information regarding the products or services at risk and appropriate precautions available to minimize risks. Until the cyber security incident has been corrected, the vendor could be requested to perform analysis of information available or obtainable, provide an action plan, provide ongoing status reports, mitigating controls, and final resolution within reasonable periods as agreed on by vendor and Responsible Entity.

[4] An example set of baseline supply chain cyber security procurement language for use by BES owners, operators, and vendors during the procurement process can be obtained from the "Cybersecurity Procurement Language for Energy Delivery Systems" developed by the Energy Sector Control Systems Working Group (ESCSWG).

1.2.3. *Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;*

- In an RFP or during contract negotiations, request that the vendor include in the contract provisions an obligation for the vendor to provide notification to the Responsible Entity when vendor employee remote or onsite access should no longer be granted. This does not require the vendor to share sensitive information about vendor employees. Circumstances for no longer granting access to vendor employees include: (i) vendor determines that any of the persons permitted access is no longer required, (ii) persons permitted access are no longer qualified to maintain access, or (iii) vendor's employment of any of the persons permitted access is terminated for any reason. Request vendor cooperation in obtaining Responsible Entity notification within a negotiated period of time of such determination. The vendor and Responsible Entity should define alternative methods that will be implemented in order to continue ongoing operations or services as needed.
- If vendor utilizes third parties (or subcontractors) to perform services to Responsible Entity, require vendors to obtain Responsible Entity's prior approval and require third party's adherence to the requirements and access termination rights imposed on the vendor directly.

1.2.4. *Disclosure by vendors of known vulnerabilities;*

- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor for cooperation in obtaining access to summary documentation within a negotiated period of any identified security breaches involving the procured product or its supply chain that impact the availability or reliability of the Responsible Entity's BES Cyber System. Documentation should include a summary description of the breach, its potential security impact, its root cause, and recommended corrective actions involving the procured product.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor for cooperation in obtaining, within a negotiated time period after establishing appropriate confidentiality agreement, access to summary documentation of uncorrected security vulnerabilities in the procured product that have not been publicly disclosed. The summary documentation should include a description of each vulnerability and its potential impact, root cause, and recommended compensating security controls, mitigations, and/or procedural workarounds.
- During procurement, review with the vendor summary documentation of publicly disclosed vulnerabilities in the product being procured and the status of the vendor's disposition of those publicly disclosed vulnerabilities.

1.2.5. *Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System; and*

- During procurement, request access to vendor documentation detailing the vendor patch management program and update process for all system components being procured (including third-party hardware, software, and firmware). This documentation should include the vendor's method or recommendation for how the integrity of the patch is validated by Responsible Entity. Ask vendors to describe the processes they use for delivering software and the methods that can be used to verify the integrity and authenticity of the software upon receipt, including systems with preinstalled software.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor to provide access to vendor documentation for the procured products (including third-party hardware, software, firmware, and services) regarding the release schedule and availability of updates and patches that should be considered or applied. Documentation should include instructions for securely applying, validating and testing the updates and patches.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor to provide appropriate software and firmware updates to remediate newly discovered vulnerabilities or weaknesses within a reasonable period for duration of the product life cycle. Consideration regarding service level agreements for updates and patches to remediate critical vulnerabilities should be a shorter period than other updates. If updates cannot be made available by the vendor within a reasonable period, the vendor should be required to provide mitigations and/or workarounds.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor to provide fingerprints or cipher hashes for all software so that the Responsible Entity can verify the values prior to installation on the BES Cyber System to verify the integrity of the software.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor such that when third-party software components are provided by the vendor, the vendors provide appropriate updates and patches to remediate newly discovered vulnerabilities or weaknesses of the third-party software components.

1.2.6. *Coordination of controls for vendor-initiated remote access.*

- During procurement, request vendors specify specific IP addresses, ports, and minimum privileges required to perform remote access services.
- Request vendors use individual user accounts that can be configured to limit access and permissions.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor to maintain their IT assets (hardware, software and firmware) connecting to Responsible Entity network with current updates to remediate security vulnerabilities or weaknesses identified by the original OEM or Responsible Entity.
- During procurement, request vendors document their processes for restricting connections from unauthorized personnel. Vendor personnel are not authorized to disclose or share account credentials, passwords or established connections.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor such that for vendor system-to-system connections that may limit the Responsible Entity's capability to authenticate the personnel connecting from the vendor's systems, the vendor will maintain complete and accurate books, user logs, access credential data, records, and other information applicable to connection access activities for a negotiated time period.

Requirement R2

R2. *Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1.*

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

General Considerations for R2

Implementation of the supply chain cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders), consistent with Order No. 829 (P. 36). Contracts entering the Responsible Entity's procurement process (e.g. through Request for Proposals) on or after the effective date are within scope of CIP-013-2. Contract effective date, commencement date, or other activation dates specified in the contract do not determine whether the contract is within scope of CIP-013-2.

Requirement R3

R3. *Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months.*

General Considerations for R3

In the Requirement R3 review, responsible entities should consider new risks and available mitigation measures, which could come from a variety of sources that include NERC, DHS, and other sources.

Implementation Guidance for R3

Responsible entities use various processes to address this requirement. Below are some examples of approaches to comply with this requirement:

- A team of subject matter experts from across the organization representing appropriate business operations, security architecture, information communications and technology, supply chain, compliance, legal, etc. reviews the supply chain cyber security risk management plan at least once every 15 calendar months to reassess for any changes needed. Sources of information for changes include, but are not limited to:
  - Requirements or guidelines from regulatory agencies
  - Industry best practices and guidance that improve supply chain cyber security risk management controls (e.g. NERC, DOE, DHS, ICS-CERT, Canadian Cyber Incident Response Center (CCIRC), and NIST).
  - Mitigating controls to address new and emerging supply chain-related cyber security concerns and vulnerabilities
  - Internal organizational continuous improvement feedback regarding identified deficiencies, opportunities for improvement, and lessons learned.
- The CIP Senior Manager, or approved delegate, reviews any changes to the supply chain cyber security risk management plan at least once every 15 calendar months. Reviews may be more frequent based on the timing and scope of changes to the supply chain cyber security risk management plan(s). Upon approval of changes to the supply chain cyber security risk management plan(s), the CIP Senior Manager or approved delegate should provide appropriate communications to the affected organizations or individuals. Additionally, communications or training material may be developed to ensure any organizational areas affected by revisions are informed.

References

- Utilities Technology Council (UTC) "Cyber Supply Chain Risk management for Utilities – Roadmap for Implementation"
- ISO/IEC 27036 – Information Security in Supplier Relationships
- NIST SP 800-53 - Security and Privacy Controls for Federal Information Systems and Organizations System and Services Acquisition SA-3, SA-8 and SA-22
- NIST SP 800-161 - Supply Chain Risk Management Practices for Federal Information Systems and Organizations;
- Energy Sector Control Systems Working Group (ESCSWG) - "Cybersecurity Procurement Language for Energy Delivery Systems"