NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT

Cyber Security — Physical Security of BES Cyber Systems

Technical Rationale and Justification for Reliability Standard CIP-006-7

January 2021

RELIABILITY | RESILIENCE | SECURITY




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

Table of Contents

Technical Rationale for Reliability Standard CIP-006-7

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-006-7. 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-006-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received addressing the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale" document for reference when reading the technical rational that follows.

Requirement R1 – Requirement R3

Rationale

Shared Cyber Infrastructure (SCI) is mutually exclusive from BES Cyber System (BCS) by definition. To enable CIP-006-7 for virtualization, SDT added SCI and matched it to the BCS already listed in Applicable Systems.

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-006-7 to align Physical Security of BES Cyber System (BCS) requirements with the virtualization changes. The conforming changes are as follows:

Applicable Systems containing High Impact BCS:

- Where the former Applicable Systems included High Impact BES Cyber Systems and their associated EACMS and PCA, the conforming change includes adding SCI to the applicability to match the existing High impact BCS and includes, "SCI hosting High Impact BCS or their associated EACMS or PCA." Affected Requirement Parts are:
  - Requirement R1 Part 1.3
  - Requirement R1 Part 1.4
  - Requirement R1 Part 1.5
  - Requirement R1 Part 1.8
  - Requirement R1 Part 1.9
  - Requirement R2 Part 2.1
  - Requirement R2 Part 2.2
  - Requirement R2 Part 2.3

Applicable Systems containing a variant of Medium Impact BCS:

- Where the former Applicable Systems included Medium Impact BES Cyber Systems without ERC, the conforming change is adding "SCI hosting..." Affected Requirement Part is:
  - Requirement R1 Part 1.1

- Where the former Applicable Systems included Medium Impact BES Cyber Systems with External Routable Connectivity and their associated EACMS and PCA, the conforming change is adding SCI to the applicability to match the updated Medium impact BCS and includes, "SCI, with ERC, hosting Medium Impact BCS or their associated EACMS or PCA." Affected Requirement Parts are:
  - Requirement R1 Part 1.2
  - Requirement R1 Part 1.4
  - Requirement R1 Part 1.5
  - Requirement R1 Part 1.8
  - Requirement R1 Part 1.9
  - Requirement R2 Part 2.1
  - Requirement R2 Part 2.2
  - Requirement R2 Part 2.3

Applicable Systems containing a variant of Physical Access Control Systems (PACS):

- Where the former Applicable Systems included Physical Access Control Systems (PACS) associated with High Impact BES Cyber Systems, the SDT added SCI to match the existing BCS by including "SCI hosting High Impact BCS"; Here, the SDT also extended SCI hosting applicability to the High Impact BCS's associated EACMS or PCA. CIP-006-7 contains several Requirement Parts where the target of the control includes the PACS themselves. In this case, the SDT determined the appropriate PACS to protect would be those that secure the Applicable Systems of Requirement R1 Parts 1.2 & 1.3. The SDT is constrained by the current SAR to only apply these updates to the virtualized versions of those targets, which resulted in the various "SCI hosting…" bullets included under PACS, as well as the SCI hosting PACS references within the applicability of these requirements." Lastly, the SDT added a separate entry for "SCI hosting PACS associated with High Impact BCS"
    - Requirement R1 Part 1.1
    - Requirement R1 Part 1.6
    - Requirement R1 Part 1.7
    - Requirement R3 Part 3.1

- Where the former Applicable Systems included Physical Access Control Systems (PACS) associated with Medium Impact BES Cyber Systems with ERC, the SDT added SCI to match the existing BCS by including "SCI hosting High Impact BCS"; Here, the SDT also extended SCI hosting applicability to the associated EACMS or PCA of the Medium impact BCS with ERC. CIP-006-7 contains several Requirement Parts where the target of the control includes the PACS themselves. In this case, the SDT determined the appropriate PACS to protect would be those that secure the Applicable Systems of Requirement R1 Parts 1.2 & 1.3. The SDT is constrained by the current SAR to only apply these updates to the virtualized versions of those targets, which resulted in the various "SCI hosting…" bullets included under PACS, as well as the SCI hosting PACS references within the applicability of these requirements." Lastly, the SDT added a separate entry for "SCI hosting PACs associated with Medium Impact BCS with ERC".
    - Requirement R1 Part 1.1
    - Requirement R1 Part 1.6
    - Requirement R1 Part 1.7
    - Requirement R3 Part 3.1

Applicable Systems containing Locally mounted hardware or devices at the Physical Security Perimeter (PSP):

- Where the former Applicable Systems included locally mounted hardware with associated with High Impact BES Cyber Systems, the SDT added SCI to match the existing BCS by including "SCI hosting PACS associated with High Impact BCS". Affected Requirement Part is:
    - Requirement R3 Part 3.1
- Where the former Applicable Systems included locally mounted hardware associated with Medium Impact BES Cyber Systems with External Routable Connectivity, "the SDT added SCI to match the existing BCS by including "SCI hosting PACs associated with Medium Impact BCS with ERC." Affected Requirement Part is:
    - Requirement R3 Part 3.1

Other modifications:

- The SDT also evaluated where CIP Exceptional Circumstances (CEC) should be included, and has added this provision to the following requirement parts:
  - Requirement R1 Part 1.8.

    Rationale: Responsible Entities may not be able to log entry of each individual with authorized unescorted physical access into each Physical Security Perimeter if a facility that contains the Physical Security Perimeter or Physical Access Control System is damaged or destroyed.
  - Requirement R1 Part 1.9.

    Rationale: Responsible Entities may not be able to retain access logs of entry of individuals into each Physical Security Perimeter if a facility that contains the Physical Security Perimeter or Physical Access Control System is damaged or destroyed.
  - Requirement R2.

    Rationale: Responsible Entities may not be able to implement the documented visitor control program during certain conditions that qualify as CIP Exceptional Circumstances. Conditions could include a risk of injury or death, a natural disaster that damages or destroys a Responsible Entity's facilities, or first responders the require access to the Physical Security Perimeter.
- The SDT chose to remove the reliance on a Technical Feasibility in favor of the updated term “per system capability.”
  - Requirement R1 Part 1.3.

    Rationale: The SDT contends that the term still requires an entity to document the limit to the system’s capability with regards to the requirement language, while not incurring the additional documentation overhead of a Technical Feasibility Exception.
- The SDT deleted Requirement R1 Part 1.10 from CIP-006-7 because it is incorporated into CIP-005-8 Requirement R1 Part 1.3.

Former Background Section from Reliability Standard CIP-006-6

The section **6. Background** has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-006 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems without External Routable Connectivity** – Only applies to medium impact BES Cyber Systems without External Routable Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

Technical Rational for Reliability Standard CIP-006-6

This section contains a "cut and paste" of the former Guidelines and Technical Basis (GTB) as-is of from CIP-006-6 standard to preserve any historical references. No modifications have been made.

Guidelines and Technical Basis

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.

General:

While the focus of this Reliability Standard has shifted away from the definition and management of a completely enclosed "six-wall" boundary, it is expected that in many instances a six-wall boundary will remain a primary mechanism for controlling, alerting, and logging access to BES Cyber Systems. Taken together, these controls outlined below will effectively constitute the physical security plan to manage physical access to BES Cyber Systems.

Requirement R1:

Methods of physical access control include:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.

- Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.
- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access into the Physical Security Perimeter.

Methods to monitor physical access include:

- Alarm Systems: Systems that alarm to indicate interior motion or when a door, gate, or window has been opened without authorization. These alarms must provide for notification within 15 minutes to individuals responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by security personnel who are also controlling physical access.

Methods to log physical access include:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and alerting method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access.

The FERC Order No. 706, Paragraph 572, directive discussed utilizing two or more different and complementary physical access controls to provide defense in depth. It does not require two or more Physical Security Perimeters, nor does it exclude the use of layered perimeters. Use of two-factor authentication would be acceptable at the same entry points for a non-layered single perimeter. For example, controls for a sole perimeter could include either a combination of card key and pin code (something you know and something you have), or a card key and biometric scanner (something you have and something you are), or a physical key in combination with a guard-monitored remote camera and door release, where the "guard" has adequate information to authenticate the person the guard is observing or talking to prior to permitting access (something you have and something you are). The two-factor authentication could be implemented using a single Physical Access Control System but more than one authentication method must be utilized. For physically layered protection, a locked gate in combination with a locked control-building could be acceptable, provided no single authenticator (e.g., key or card key) would provide access through both.

Entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement Parts 1.1, 1.6 and 1.7 beyond what is already required for the PSP.

The new requirement part CIP-006-6, Requirement R1, Part 1.10 responds to the directive found in FERC Order No. 791, Paragraph 150. The requirement intends to protect cabling and

nonprogrammable communication components that are within an ESP, but extend outside of a PSP. This protection, similar to the FERC Approved NERC Petition on the interpretation on CIP-006-2 from PacifiCorp, must be accomplished either by physically protecting the cabling and components that leave a PSP (such as by conduit or secured cable trays) or through data encryption, circuit monitoring, or equally effective logical protections. It is intended that the physical protections reduce the possibility of tampering or allowing direct access to the nonprogrammable devices. Conduit, secured cable trays, and secured communication closets are examples of these types of protections. These physical security measures should be implemented in such a way that they would provide some mechanism to detect or recognize that someone could have tampered with the cabling and non-programmable components. This could be something as simple as a padlock on a communications closet where the entity would recognize if the padlock had been cut off. Alternatively, this protection may also be accomplished through the use of armored cabling or via the stainless steel or aluminum tube protecting the fiber inside an optical ground wire (OPGW) cable. In using any of these methods, care should be taken to protect the entire length of the cabling including any termination points that may be outside of a defined PSP.

This requirement part only covers those portions of cabling and nonprogrammable communications components that are located outside of the PSP, but inside the ESP. Where this cabling and non-programmable communications components exist inside the PSP, this requirement part no longer applies.

The requirement focuses on physical protection of the communications cabling and components as this is a requirement in a physical security standard and the gap in protection identified by FERC in Order 791 is one of physical protections. However, the requirement part recognizes that there is more than one way to provide protection to communication cabling and nonprogrammable components. In particular, the requirement provides a mechanism for entities to select an alternative to physical security protection that may be chosen in a situation where an entity cannot implement physical security or simply chooses not to implement physical security. The entity is under no obligation to justify or explain why it chose logical protections over physical protections identified in the requirement.

The alternative protective measures identified in the CIP-006-6 R1, Part 1.10 (encryption and circuit monitoring) were identified as acceptable alternatives in NERC petition of the PacifiCorp Interpretation of CIP-006-2 which was approved by FERC (RD10-13-000). If an entity chooses to implement an “an equally effective logical protection” in lieu of one of the protection mechanisms identified in the standard, the entity would be expected to document how the protection is equally effective. NERC explained in its petition of the PacifiCorp Interpretation of CIP-006-2 that the measures are relevant to access or physical tampering. Therefore, the entity may choose to discuss how its protection may provide detection of tampering. The entity may also choose to explain how its protection is equivalent to the other logical options identified in the standard in terms of the CIA triad (confidentiality, integrity, and availability). The entity may find value in reviewing their plans prior to implementation with the regional entity, but there is no obligation to do so.

The intent of the requirement is not to require physical protection of third party components, consistent with FERC Order 791-A. The requirement allows flexibility in that the entity has control of how to design its ESP and also has the ability to extend its ESP outside its PSP via the logical mechanisms specified in CIP-006-6 Requirement 1, Part 1.10 such as encryption (which is an option specifically identified in FERC Order 791-A). These mechanisms should provide sufficient protections to an entity's BES Cyber Systems while not requiring controls to be implemented on third-party components when entities rely on leased third-party communications.

In addition to the cabling, the components in scope of this requirement part are those components outside of a PSP that could otherwise be considered a BES Cyber Asset or Protected Cyber Asset except that they do not meet the definition of Cyber Asset because they are nonprogrammable. Examples of these nonprogrammable components include, but are not limited to, unmanaged switches, hubs, patch panels, media converters, port savers, and couplers.

Requirement R2:

The logging of visitors should capture each visit of the individual and does not need to capture each entry or exit during that visit. This is meant to allow a visitor to temporarily exit the Physical Security Perimeter to obtain something they left in their vehicle or outside the area without requiring a new log entry for each and every entry during the visit.

The SDT also determined that a point of contact should be documented who can provide additional details about the visit if questions arise in the future. The point of contact could be the escort, but there is no need to document everyone that acted as an escort for the visitor.

Requirement R3:

This includes the testing of locally mounted hardware or devices used in controlling, alerting or logging access to the Physical Security Perimeter. This includes motion sensors, electronic lock control mechanisms, and badge readers which are not deemed to be part of the Physical Access Control System but are required for the protection of the BES Cyber Systems.

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:

Each Responsible Entity shall ensure that physical access to all BES Cyber Systems is restricted and appropriately managed. Entities may choose for certain Physical Access Control Systems (PACS) to reside in a Physical Security Perimeter (PSP) controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement R1, Parts 1.1, 1.6 and 1.7 beyond what is already required for the PSP.

Regarding Requirement R1, Part 1.10, when cabling and other nonprogrammable components of a Control Center's communication network cannot be secured in a PSP, steps must be taken to ensure the integrity of the BES Cyber Systems. Exposed communication pathways outside of a PSP necessitate that physical or logical protections be installed to reduce the likelihood that

man-in-the-middle attacks could compromise the integrity of their connected BES Cyber Assets or PCAs that are required to reside within PSPs. While it is anticipated that priority consideration will be given to physically securing the cabling and nonprogrammable communications components, the SDT understands that configurations arise when physical access restrictions are not ideal and Responsible Entities are able to reasonably defend their physically exposed communications components through specific additional logical protections.

Rationale for Requirement R2:

To control when personnel without authorized unescorted physical access can be in any Physical Security Perimeters protecting BES Cyber Systems or Electronic Access Control or Monitoring Systems, as applicable in Table R2.

Rationale for Requirement R3:

To ensure all Physical Access Control Systems and devices continue to function properly.