NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security — Information Protection

Technical Rationale and Justification for Reliability Standard CIP-011-3

August 2020

RELIABILITY | RESILIENCE | SECURITY




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

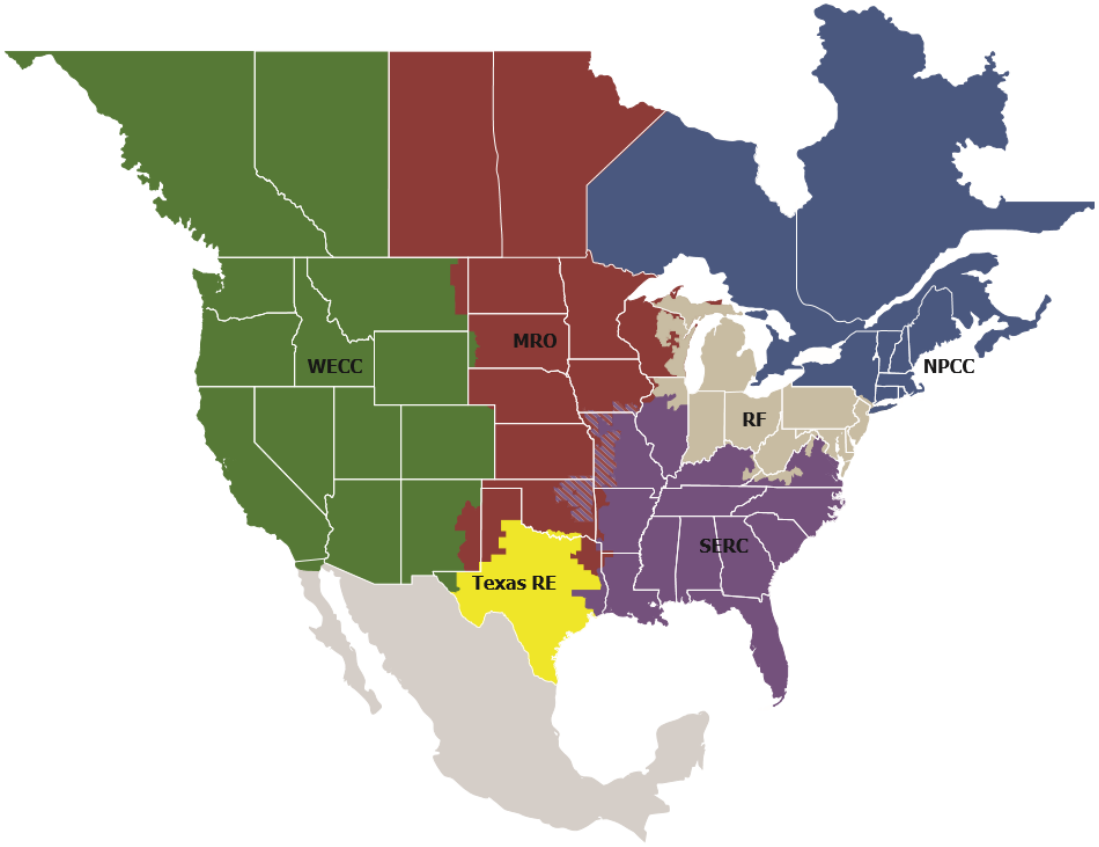
Table of Contents

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

Background

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-011-3. 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 the standard drafting team's (SDT's) intent in drafting the requirements. This Technical Rationale and Justification for CIP-011-3 is not a Reliability Standard and should not be considered mandatory and enforceable.

On July 24, 2019, the North American Electric Reliability Corporation (NERC) Standards Committee accepted a Standard Authorization Request (SAR) approving an initiative to enhance BES reliability by creating increased choice, greater flexibility, higher availability, and reduced-cost options for entities to manage their BES Cyber System Information (BCSI), by providing a secure path towards utilization of modern third-party data storage and analysis systems. In addition, the project intended to clarify the protections expected when utilizing third-party solutions (e.g., cloud services).

In response to this SAR, the Project 2019-02 SDT drafted Reliability Standard CIP-011-3 to require Responsible Entities to implement specific controls in Requirement R1 and Requirement R2 for procedural and technical controls related to BCSI during storage, handling, use, and disposal when implementing vendor provided services such as Software as a Service (SaaS), Infrastructure as a Service (IaaS), or Platform as a Service (PaaS).

New and Modified Terms Used on NERC Reliability Standards

Proposed Modified Terms:

None

Proposed New Terms:

None

Rationale for Applicability Section

Standard CIP-011 has been modified to enhance protection of BCSI. The modified requirements under CIP-011 address protection of information in several facets that are discussed in this document, which include the following:

- Modifying the "Applicable Systems" column to "Applicability" where appropriate to specifically include BCSI
- Implement methods to identify risks involving vendor services related to BCSI
- Implement technical mechanisms to protect BCSI when engaging vendor services

To provide clarity, the Applicability Systems column, which now contains BCSI, is included to associate the requirement and address the focus on protecting the BCSI regardless of the location of the BCSI. In addition, the title of the column is "Applicability" to accommodate this philosophical change.

Requirement R1

General Considerations for Requirement R1

None

Rationale for Requirement R1:

Requirement R1 specifies procedural and technical controls for BCSI handling during storage, transit, use, and disposal including implementation of vendor-provided services such as Software as a Service (SaaS), Infrastructure as a Service (IaaS), or Platform as a Service (PaaS).

Requirement R1, Part 1.1, is intended to identify BCSI and provide documented methods to support this identification process.

The SDT clarified the intent of addressing BCSI as opposed to the BES Cyber System with associated applicable systems, which may contain BCSI. The Applicable Systems column includes language to specify BCSI "…pertaining to" the applicable systems. In addition, the title of the column is "Applicability" to accommodate this philosophical change.

Rationale for Modifications to Requirement R1, Part 1.2

Requirement R1, Part 1.2, addresses methods to protect BCSI. Different states of information from the requirement; such as "transit" or "storage" are removed. The intent is to reduce confusion of Responsible Entities attempting to interpret controls specific to different states of information, limiting controls to said states, overlapping controls between states, and reduce confusion from an enforcement perspective. By removing this language, methods to protect BCSI becomes explicitly comprehensive.

Requirement language revisions reflect consistency with other CIP requirements.

Rationale for New Requirement R1, Part 1.3

Requirement R1, Part 1.3, addresses the need for the Responsible Entity to understand details of the vendor's service environment and the vendor's controls where the entity's BCSI would be stored. This requirement contains technical detail specifically on the protection of BCSI. This is inherently different than CIP-013's overall risk approach to applicable systems and vendor-contracted relationships. This requirement is for implementing risk identification and assessment methods for the following sub requirements:

- Data governance and rights management
- Identity and access management
- Security management
- Application, infrastructure, and network security

Implemented identification and assessment methods are needed to understand the risks to BCSI when choosing to engage vendor services. It is important that the Responsible Entity conducts such due diligence to understand the risks related to the vendor's environment and controls given the compromise of BCSI involves critical infrastructure and recovery from compromise may be difficult due to the duration of remediation and related remediation costs. This is different than many other industries that are capable of superseding compromised information in a relatively short period of time. There are risks that cannot be mitigated directly in the vendor environment due to the lack of Responsible Entity control. This requirement ensures that, prior to BCSI entering a vendor's environment, the

Responsible Entity is well informed regarding the vendor's environment and controls and influences what, if any, varying controls offered by a vendor are utilized, or may influence the Responsible Entity's use of technical mechanisms (see CIP-011, R1.4) for which the Responsible Entity has more control.

The intent of addressing BCSI is clarified as opposed to the BES Cyber System with associated applicable systems, which may contain BCSI; the Applicable Systems column includes language to specify BCSI that is pertinent with associated applicable systems. In addition, the title of the column is "Applicability" to accommodate this philosophical change.

The SDT's intent of the information protection program is to protect BCSI.

Responsible Entities are free to utilize existing change management and asset management systems. However, the information contained within those systems must be evaluated, as the information protection requirements still apply.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

This requirement mandates that BCSI be identified. The Responsible Entity has flexibility in determining how to implement the requirement.

The SDT does not intend that this requirement cover publicly available information, such as vendor manuals that are available via public websites or information that is deemed to be publicly releasable.

Information protection pertains to both digital and hardcopy information. Part 1.2 requires one or more methods for the protection and secure handling of BCSI. This includes information that may be stored on Transient Cyber Assets or Removable Media.

It is not the intent of this standard to mandate the use of one particular format for secure handling during transit of BCSI.

Rationale for New Requirement R1, Part 1.4:

The SDT's intent of the information protection program is to protect BCSI.

Requirement R1, Part 1.4, specifies technical, logical controls for the protection of electronic BES Cyber System Information during storage, transit, use, and disposal when implementing vendor-provided services such as SaaS, IaaS, or PaaS.

Requirement R1, Part 1.4, requires Responsible Entities to implement technical mechanisms to protect BCSI when engaging vendor services. Technical mechanisms provide a layer of defense against compromise needed to ensure a vendor's staff might have the means to electronically obtain BCSI but not use or modify BCSI. Technical mechanisms to protect BCSI are needed regardless of the location or state in which the Responsible Entity's BCSI resides when using vendor services. This requirement compliments R1, Part 1.3. Once, the risks are identified, appropriate technical mechanisms can be used to protect BCSI.

The intent of addressing BCSI is clarified as opposed to the BES Cyber System with associated applicable systems, which may contain BCSI. The Applicability column accommodates this philosophical change and to be consistent with the Applicability language added in Requirement R1, Parts 1.2 through 1.4.

Requirement R2

General Considerations for Requirement R2

None

Rationale for Requirement R2:

The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BCSI upon reuse or disposal.

This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

Requirement 3 has remained unchanged. The requirements are focused more on the reuse and disposal of BCS rather than BCSI. While acknowledging that such BCS and other applicable systems may have BCSI residing on them, the original intent of the requirement is broader than addressing BCSI. This is a lifecycle issue concerning the applicable systems. CIP-002 focuses on the beginning of the BCS lifecycle but not an end. The potential end of the applicable systems lifecycle is absent from CIP-011 to reduce confusion with reuse and disposal of BCSI. The 2019 BCSI Access Management project did not include modification of CIP-002 in the scope of the SAR. This concern has been communicated for future evaluation.

Technical Rationale for Reliability Standard CIP-011-2

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-011-2 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:

Responsible Entities are free to utilize existing change management and asset management systems. However, the information contained within those systems must be evaluated, as the information protection requirements still apply.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

This requirement mandates that BES Cyber System Information be identified. The Responsible Entity has flexibility in determining how to implement the requirement.

The SDT does not intend that this requirement cover publicly available information, such as vendor manuals that are available via public websites or information that is deemed to be publicly releasable.

Information protection pertains to both digital and hardcopy information. R1.2 requires one or more procedures for the protection and secure handling BES Cyber System Information, including storage, transit, and use. This includes information that may be stored on Transient Cyber Assets or Removable Media.

It is not the intent of this standard to mandate the use of one particular format for secure handling during transit.

Requirement R2:

This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

Rationale:

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

Rationale for Requirement R1:

The SDT's intent of the information protection program is to prevent unauthorized access to BES Cyber System Information.

Rationale for Requirement R2:

The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BES Cyber System Information upon reuse or disposal.