NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Technical Rationale for Reliability Standard CIP-011-3

December 2019

CIP-011-3 – Information Protection

Rationale for Applicability Section
Standard CIP-011 has been modified to enhance protection of BES Cyber System Information (BCSI). The modified requirements under CIP-011 will address protection of information in several facets that are discussed in this document, which include the following:

- Identification of BCSI
- Prevention of unauthorized access to BCSI
- Authorization of approved access to BCSI
- Risk assessments for BCSI not stored in the Responsible Entity's environment
- Termination of access to BCSI
- Review of access BCSI
- Key management to restrict access to BCSI
- Controls to separate duties for protecting BCSI

To provide clarity, the Applicability Systems column, which now contains BCSI, was 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 has been changed to "Applicability" to accommodate this philosophical change.

To address access-management-related requirements for BCSI, the related requirements from CIP-004-6 (Requirement R4, Parts 4.1.3 and 4.4, and Requirement R5, Part 5.3) have been transferred to CIP-011. This allows CIP-011 to become a more mature and easier standard to follow and update for future modifications.

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

The standard drafting team (SDT) clarified the intent of addressing BCSI as opposed to the BES Cyber System (BCS) with associated applicable systems, which may contain BCSI; the Applicable Systems column

has added language to specify system information that is affiliated with High Impact and Medium Impact BES Cyber Systems and their associated applicable systems. In addition, the title of the column has been changed to "Applicability" to accommodate this philosophical change.

Protected Cyber Assets were added to the Applicability column to ensure system information pertaining to Protected Cyber Assets is reviewed within the Responsibility Entity's information protection program subject to CIP-011 requirements, which was not previously required. Protected Cyber Assets are also applicable to CIP-011-3, Requirement R1, Parts 1.2 through 1.6, and CIP-011-3, Requirement R2, Parts 2.1 and 2.2.

Requirement language was added to Requirement R1, Part 1.1, to identify designated BCSI storage locations, whether physical or electronic. This identification should be as follows:

1) Defined as a friendly name of the electronic or physical repository (thus protecting the actual storage location); and
2) The description of the storage location (e.g., physical or electronic, off-premises or on premises).

The SDT wanted to ensure access management controls were focused on access to BCSI rather than access to BCSI designated storage locations. If a BCSI designated storage location was not identified because it does not exist, this would provide a means of accounting and clarifying this potential scenario.

The SDT has intentionally not included Low Impact BCS and their associated systems in CIP-011. Requirement R1, Part 1.1, only includes High Impact and Medium Impact BCS and their associated systems (PACS, EACMS, and PCA). The SDT also referenced Requirement R1, Part 1.1, in the Applicability column of Requirement R1, Parts 1.2 through 1.6, and Requirement R2, Parts 2.1 and 2.2, so the Responsible Entity can easily determine the applicability of those sub-requirements based on how the Responsible Entity defined and identified BCSI to satisfy Requirement R1, Part 1.1. This further clarifies there is no CIP-011 applicability to Low Impact BCS and their associated systems.

Rationale for Modifications to Requirement R1, Part 1.2

Requirement R1, Part 1.2, addresses protecting and securely handling BCSI throughout its life cycle. This life cycle includes creation, use, exchange or sharing (i.e., transit), storage, and disposal. A key component of the information protection of BCSI is the secure handling of BCSI during each of these life cycle phases.

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 has added language to specify BCSI that is affiliated with associated applicable systems. In addition, the title of the column has been changed to "Applicability" to accommodate this philosophical change.

Language was added to incorporate the NERC CMEP Practice Guide where BCSI access is defined as the ability to obtain and use BCSI.

Requirement language was revised to reflect consistency with other CIP requirements as well as the current rationale for CIP-011-2, Requirement R1 (e.g., prevent unauthorized access).

Requirement language was added to include disposal as part of the BCSI life cycle. While it is assumed that disposal of BCSI is part of the BCSI life cycle, it was not previously required.

Rationale for New Requirement R1, Part 1.3
New Requirement R1, Part 1.3, was transferred from CIP-004-6, Requirement R4, Part 4.1.3, to consolidate into one Standard both BCSI protection and access authorization to BCSI.

The SDT wanted to separate the concept of protecting information via a physical device or location from protecting the information (BCSI) itself. If the focus is protection of BCSI, the device or storage location becomes less relevant. This is important when considering vendor storage as a service and security considerations regarding physical access and information moving between physical devices outside of the Responsible Entity's direct control. To accomplish this, the focus and means of protection have been shifted to address the possession and utilization of the information. Possession of BCSI addresses physical and electronic/digital controls to protect BCSI. Utilization of BCSI addresses that when BCSI is not in possession, an entity can take precautions to reasonably assure that, if BCSI is compromised from a possession aspect, the BCSI would not be able to be utilized. There are three benefits with moving in this direction:

1) There are different levels of compromise. This provides a more granular way of evaluating and reporting risk during a BCSI compromise. Before this approach, reporting a compromise or mishandling was binary and did not accurately depict risk or the actual ability of a threat actor to capitalize and exploit the information.
2) The focus is now on ensuring controls around BCSI. Physical and electronic controls now become a means to protect how information is possessed and utilized.
3) There is now the ability for the entity to address controls that are independent of possession of BCSI. This will play a significant role in leveraging technologies such as the "cloud."

The SDT also wanted to ensure backwards compatibility with the previous requirement, where feasible. Authorization for electronic and unescorted physical access and access to BCSI must still be based on necessity of the individual performing a work function. Documentation showing the authorization should still have some justification of the business need included. To ensure proper segregation of duties, the same person should still not perform access authorization and provisioning, where possible.

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 has added language to specify BCSI that is affiliated with associated applicable systems. In addition, the title of the column has been changed to "Applicability" to accommodate this philosophical change.

Rationale for New Requirement R1, Part 1.4
New Requirement R1, Part 1.4, was drafted to allow Responsible Entities to implement a BCSI risk management methodology for vendors that store the Responsible Entity's BCSI and allow a risk-based approach to address the security objectives. One example of a risk-based approach is allowing Responsible Entities to develop their BCSI risk management methodology around risks posed by various vendors involved within the Responsible Entity's BCSI life cycle. This flexibility is important to account for the varying needs and characteristics of Responsible Entities and the diversity of BCSI-related environments, technologies, and risk.

The SDT recognized that CIP-013-1, Requirement R1, can be leveraged to incorporate protection of BCSI but does not currently include information protection.

This requirement includes the following three sub-requirements as a basis for implementing a BCSI risk management methodology:

1) Part 1.4.1 is included so the Responsible Entity will perform an initial risk assessment of any vendor(s) selected to store its BCSI to identify risk factors that could potentially compromise the Responsible Entity's BCSI within the vendor's environment, analyze the risk of the BCSI being compromised, and review the results of the risk analysis.
2) Part 1.4.2 is included so the Responsible Entity will review the vendor(s) that stores its BCSI at least every 15 calendar months to confirm whether the vendor(s) is still the most reliable vendor to perform that function for the Responsible Entity and the Bulk Electric System.
3) Part 1.4.3 is included so the Responsible Entity will document the results from the risk assessments performed in Parts 1.4.1 and 1.4.2 and an action plan to remediate or mitigate risks identified in the assessment.

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 has added language to specify BCSI that is affiliated with associated applicable systems. In addition, the title of the column has been changed to "Applicability" to accommodate this philosophical change.

Rationale for New Requirement R1, Part 1.5
New Requirement R1, Part 1.5, was transferred from CIP-004-6, Requirement R5, Part 5.3, to consolidate into one Standard both BCSI protection and BCSI access revocation for termination actions within 24 hours.

The SDT wanted to ensure backwards compatibility with the previous requirement, where feasible. The requirement to revoke access to BCSI at the time of the termination action still includes procedures showing revocation of access to BCSI concurrent with the termination action. This requirement also still recognizes the timing of the termination action might vary depending on the circumstance.

For applicability, the SDT included Medium Impact BES Cyber Systems with this requirement regardless of whether the Medium Impact BES Cyber System had External Routable Connectivity. The SDT does not

feel that External Routable Connectivity is a determining factor for what the Responsible Entity has identified as BCSI.

Revocation of electronic access is still understood to mean a process with the result that electronic access to BCSI is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked. Steps taken to accomplish this outcome may include deletion or deactivation of accounts used by the individual(s), but no specific actions are prescribed. Responsible Entities should still consider the ramifications of deleting an account might include incomplete event log entries due to an unrecognized account or system services using the account to log on.

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 has added language to specify BCSI that is affiliated with associated applicable systems. In addition, the title of the column has been changed to "Applicability" to accommodate this philosophical change.

Rationale for New Requirement R1, Part 1.6

New Requirement R1, Part 1.6, was transferred from CIP-004-6, Requirement R4, Part 4.4, to consolidate into one Standard both BCSI protection and the 15-calendar-month BCSI access review.

The SDT wanted to ensure backwards compatibility with the previous requirement, where feasible. The BCSI privilege review at least once every 15 calendar months is still in place to ensure an individual's associated privileges to BCSI are the minimum necessary to perform their work function (i.e., least privilege). This involves determining the specific roles with BCSI (e.g., system operator, technician, report viewer, administrator) then grouping access privileges to the role and assigning users to the role. Role-based access to BCSI does not assume any specific software, and it can be implemented by defining specific provisioning processes for each role where access group assignments cannot be performed. Role-based access permissions eliminate the need to perform the BCSI privilege review on individual accounts.

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 has added language to specify BCSI that is affiliated with associated applicable systems. In addition, the title of the column has been changed to "Applicability" to accommodate this philosophical change.

Rationale for New Requirement R2, Part 2.1

New Requirement R2, Part 2.1, was drafted by the SDT to require Responsible Entities to develop a key management process(es) within their information protection programs to restrict access with revocation ability. Key management provides a layer of defense against bad actors who may have the means to physically or electronically obtain BCSI but not use or modify BCSI; this has not been previously required but is needed regardless of the location or state in which the Responsible Entity's BCSI resides. The requirement language includes the minimum expectations for the key management life cycle to guide Responsible Entities while they are developing a key management program and to provide an auditable requirement for Compliance Enforcement Authorities.

The SDT identified the intent of addressing BCSI as opposed to the BES Cyber System with associated applicable systems, which may contain BCSI. The Applicability column has been included to accommodate this philosophical change and to be consistent with the Applicability language added in Requirement R1, Parts 1.2 through 1.6.

Rationale for New Requirement R2, Part 2.2
New Requirement R2, Part 2.2, was drafted to require Responsible Entities to ensure separation of duties in the Responsible Entity's key management process(es) so, regardless of the location or state in which the Responsible Entity's BCSI resides, the risk of unauthorized access to the Responsible Entity's BCSI can be minimized. Controls must be implemented to separate the BES Cyber System Information custodial entity's duties independently from the key management duties established in Requirement R2, Part 2.1. If a Responsibility Entity is unable to implement these controls, and there is a compromise of its BCSI, the time and cost for a Responsible Entity to recover from the compromise of its BCSI could be significant to the Responsible Entity and even to the Bulk Electric System.

The SDT identified the intent of addressing BCSI as opposed to the BES Cyber System with associated applicable systems, which may contain BCSI. The Applicability column has been included to accommodate this philosophical change and to be consistent with the Applicability language added in Requirement R1, Parts 1.2 through 1.6, and Requirement R2, Part 2.1.

Rationale for Modifications to Requirement R2, Part 2.1 (will become new Requirement R3, Part 3.1)
The SDT combined CIP-011-2, Requirement R2, Part 2.1 (reuse) and CIP-011-2, Requirement R2, Part 2.2 (disposal) within the same requirement language under CIP-011-3 Requirement R3, Part 3.1.

In addition, the phrase "that contain BES Cyber System Information" was removed from the requirement language effectively expanding applicability of sanitization or destruction practices to all Applicable Systems, not just those containing BCSI. This was done to align with the historical intent of CIP-007-3 R7 where reliability data was required to be sanitized as well from Cyber Assets before reuse or disposal.

Rationale for Retirement of CIP-011-2 Requirement R2, Part 2.2
The intent of CIP-011-2, Requirement R2, Part 2.2, which is related to BES Cyber Asset disposal, will be addressed in CIP-011-3, Requirement R3, Part 3.1, so CIP-011-2, Requirement R2, Part 2.2, is being recommended for retirement.

Technical Rationale for Reliability Standard CIP-011-2

This section contains the Guidelines and Technical basis as a "cut and paste" from CIP-011-2 standard to preserve any historical references.

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 Responsible Entity should explain the method for identifying the BES Cyber System Information in their information protection program. For example, the Responsible Entity may decide to mark or label the documents. Identifying separate classifications of BES Cyber System Information is not specifically required. However, a Responsible Entity maintains the flexibility to do so if they desire. As long as the Responsible Entity's information protection program includes all applicable items, additional classification levels (e.g., confidential, public, internal use only, etc.) can be created that go above and beyond the requirements. If the entity chooses to use

classifications, then the types of classifications used by the entity and any associated labeling should be documented in the entity's BES Cyber System Information Protection Program.

The Responsible Entity may store all of the information about BES Cyber Systems in a separate repository or location (physical and/or electronic) with access control implemented. For example, the Responsible Entity's program could document that all information stored in an identified repository is considered BES Cyber System Information, the program may state that all information contained in an identified section of a specific repository is considered BES Cyber System Information, or the program may document that all hard copies of information are stored in a secured area of the building. Additional methods for implementing the requirement are suggested in the measures section. However, the methods listed in measures are not meant to be an exhaustive list of methods that the entity may choose to utilize for the identification of BES Cyber System Information.

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.

The entity's written Information Protection Program should explain how the entity handles aspects of information protection including specifying how BES Cyber System Information is to be securely handled during transit in order to protect against unauthorized access, misuse, or corruption and to protect confidentiality of the communicated BES Cyber System Information. For example, the use of a third-party communication service provider instead of organization-owned infrastructure may warrant the use of encryption to prevent unauthorized disclosure of information during transmission. The entity may choose to establish a trusted communications path for transit of BES Cyber System Information. The trusted communications path would utilize a logon or other security measures to provide secure handling during transit. The entity may employ alternative physical protective measures, such as the use of a courier or locked container for transmission of information. It is not the intent of this standard to mandate the use of one particular format for secure handling during transit.

A good Information Protection Program will document the circumstances under which BES Cyber System Information can be shared with or used by third parties. The organization should distribute or share information on a need-to-know basis. For example, the entity may specify that a confidentiality agreement, non-disclosure arrangement, contract, or written agreement of some kind concerning the handling of information must be in place between the entity and the third party. The entity's Information Protection Program should specify circumstances for sharing of BES Cyber System Information with and use by third parties, for example, use of a non-disclosure agreement. The entity should then follow their documented program. These requirements do not mandate one specific type of arrangement.

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. However, following the analysis, if the media is to be reused outside of a BES Cyber System or disposed of, the entity must take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.

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.

If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the Responsible Entity should maintain documentation that identifies the custodian for the data storage media while the data storage media is outside of the Physical Security Perimeter prior to actions taken by the entity as required in R2.

Media sanitization is the process used to remove information from system media such that reasonable assurance exists that the information cannot be retrieved or reconstructed. Media sanitization is generally classified into four categories: Disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances, such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media that is ready for disposal.

The following information from NIST SP800-88 provides additional guidance concerning the types of actions that an entity might take to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media:

> Clear: One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method [SP 800-36].
>
> Purge: Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes. [SP 800-36] Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging.

Degaussing of any hard drive assembly usually destroys the drive as the firmware that manages the device is also destroyed.

Destroy: There are many different types, techniques, and procedures for media destruction. Disintegration, Pulverization, Melting, and Incineration are sanitization methods designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning. In some cases such as networking equipment, it may be necessary to contact the manufacturer for proper sanitization procedure.

It is critical that an organization maintain a record of its sanitization actions to prevent unauthorized retrieval of BES Cyber System Information. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes.

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 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 of a BES Cyber Asset.