NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2019-02 BES Cyber System Information Access Management

Summary Response to Comments | Draft 3

Background

Project 2019-02 BES Cyber System Information Access Management (BCSI) enhances BES reliability by creating increased choice, greater flexibility, higher availability, and reduced-cost options for entities to manage their BCSI. In addition, the project seeks to clarify the protections expected when utilizing third-party solutions (e.g., cloud services).

The Project 2019-02 BCSI standard drafting team (SDT) revised Reliability Standards CIP-004 and CIP-011 and reviewed the Glossary of Terms Used in NERC Reliability Standards pertaining to requirements addressing BCSI. The 45-day comment period was August 6 through September 21, 2020. There were 68 sets of responses, including comments from approximately 175 different people from approximately 111 companies representing 10 of the Industry Segments as shown in the table on the following pages. Based on these comments, the SDT has made proposed revisions to CIP-004 and CIP-011. Summary responses have been developed to address the comments.

CIP-004 Revisions

The SDT appreciates all comments submitted regarding the CIP-004 draft standard. The SDT reviewed each comment carefully and made respective changes where clarity or examples were needed.

Provisioned access, provisioning, deprovisioning Concepts

Many commenters expressed concern about the phrase "provisioned access, provisioning, deprovisioning" within the CIP-004 standard. Some entities recommended the term be defined or the SDT modify the requirements to provide clarity. It was also acknowledged that the Technical Rationale (TR) does a great job explaining this term, but there is concern as the TR is not enforceable.

Thank you for your comments. The SDT determined that the term provision does not need to be defined. Provision or provisioned access is a well-known term among technical subject matter experts who provision access or deprovision access as a part of their job. This is an industry proven and accepted term that aligns with security best practices and industry frameworks, which is best maintained as a non-defined term. The SDT made some modifications within the sub-requirements of CIP-004 in hopes to provide clarity around the requirements regarding provisioned access. Lastly, the SDT encourages industry to review the CIP-004-X Requirement R6 section of the TR document and use the described concepts and scenarios in written access management programs.

Storage Location

Some commenters requested that the SDT revert back to storage locations as seen in the previous approved standard. In addition, a commenter expressed conversations with the SDT have clarified that CIP-004-7 R6.1 was not intended to require provisioning of access to each individual piece of BCSI. The SDT explained that the language was written to accommodate a use case where the BCSI authorization attaches to the document so that the authorization follows the document when moved to various locations. However, the entity requested the SDT accommodate both circumstances where entities may fall under the use case scenario or may use designated storage locations for BCSI. A couple of entities expressed that the proposed language is more restrictive than objective based. Lastly, some entities are concerned that the current proposed language will not allow for backwards compatibility.

Thank you for your comments. The SDT determined that reverting back to storage locations would not be an appropriate path forward for BCSI modifications and would be a detriment for future cloud modifications to the CIP standards. The provision concept provides a clear path for BCSI and future modifications. While entities may find Requirement R6 to be more restrictive than objective, the SDT's focus is on BCSI and objective based for this specific requirement may bring more into scope than intended and would be outside the scope of this team. Lastly, using "Storage Locations" is just one method to identify and protect BCSI. The absence of "Storage Locations" does not preclude an entity from maintaining that approach as their method. Removing "Storage Locations" adds the needed flexibility for entities that want to use other approaches such as those that technologies would provide (e.g. Azure Information Protection (AIP)). The term "Storage Locations" is too prescriptive, and retention of that term encumbers the use of emerging technologies for entities that should have those methods as an option. The SDT updated the Technical Rationale (TR) with an explanation of how "provisioned access" is backwards compatible with "designated storage locations", while still also allowing certain protections (i.e. encryption) at the file level rather than all entities having to limit this to specific locations.

Applicability

Many commenters requested that the SDT revert the "Applicability" column language back to "Applicable Systems" language.

Thank you for your comments. The SDT agrees and modified the applicability column language back to "Applicable Systems."

Clarify requirements for managing provisioned access utilizing third-party solutions.

There were concerns expressed about the lack of clarity regarding Requirement R6 and what provisioned access means and the lack of clarity regarding using cloud vendors.

Thank you for your comments. The SDT reviewed requirement R6 and agrees that some modifications are necessary. Please see the modifications made to CIP-004, Requirement R6.

Requirement R6 and Subparts 6.1 and 6.2

A couple of entities expressed that Requirement R6 and its subparts do not provide clarity. The entity stated that the intent of these requirements is to manage access when utilizing third-party solutions since it doesn't explicitly make that statement. The phrase "provisioning of access" does not necessarily imply "when utilizing third-party solutions."

Thank you for your comments. The SDT chose not to differentiate between entity and third-party because the requirement applies to each individual (whether employee or non-employee) and not the hiring company nor the infrastructure solution (whether on-prem or off-prem). The intent is to keep the requirements objective and agnostic of the workforce and infrastructure. Thereby permitting entities flexibility to adapt their program to their changing environment and workforce while still meeting the security objectives and without having to revise the requirements to catch up.

Many entities expressed that management of provisioned access to BCSI, when utilizing third-party solutions, needs to be clarified. Requirement R6, part 6.1 states that entities are required to "authorize provisioning of access to BCSI based on need." This could be read to mean, among other things, that entities are required to authorize someone to provision access to BCSI, provision access to all BCSI (i.e. requiring a provisioning authorization for each piece of BCSI), or a variety of other interpretations. To resolve this issue, EEI suggests aligning the language of Requirement R6, part 6.1 to Requirement R4, part 4.1 by adding the phrase "Process to", which would place the responsibility on the entity to define its process. Additionally, if process is added to the Requirement, the entity proposes adding an example such as "A documented process used to define provisioned access to BCSI."

Thank you for your comments. The SDT's intent in this context is for "provisioned access" to be limited to what an entity's program must do (authorize, verify, and revoke) thereby permitting the entity to determine "how" provisioning occurs. "Provisioned access" is a noun that the represents the result of executing the program so the security objective is met, and not a verb relating to how provisioning/deprovisioning occurs (the provisioning/deprovisioning actions and processes are up to the entity to design within the parameters of the objective.)

An entity expressed that the addition of Requirement R6 for CIP-004 makes it extremely difficult for entities to control access to BCSI. This is because of the requirement to provision access to individual pieces of information rather than provisioning access to where information is being stored (Storage locations).

Thank you for your comments. The SDT's modifications do not prescribe how to meet the security objective, nor does it prescribe controls at the individual document level. Using "Storage Locations" is just one method that could continue to be used within an entity's access management program when it comes to authorization, verification, and revocation of access for identified BCSI. The absence of "Storage Locations" does not preclude an entity from maintaining that approach as their method. The term "Storage Locations" is too prescriptive (Removing "Storage Locations" provides flexibility), and retention of that term encumbers the use of emerging technologies and approaches for entities that should have those methods as an option in addition to (not instead of) the current method.

Some entities requested clarification whether third-party access should be managed on an individual or team basis.

Thank you for your comments. The SDT maintained objective language at the requirement level to provide entities the flexibility to define "how" access is managed. Ultimately, regardless of whether the access is provisioned on an individual or team basis, the authorization records must trace back to each individual.

There was expressed concern from some entities that Requirement R6 Part 6.1 mirrors Requirement R4 Part 4.1.

Thank you for your comments. The SDT does not agree that the new Requirement R6 Part 6.1 mirrors Requirement R4 Part 4.1. CIP-004 Requirement R4 focuses on Access Management Programs and CIP-004 Requirement R6 focuses on authorizing, verifying, and revoking provisioned access. The similarities of these requirements were intentionally drafted. The security concepts and values are comparable, but the applicability is different. While an entity may leverage one program to support the other, or produce similar evidence to demonstrate compliance, the difference between them is the existing set of requirements should focus on BCS Access Management, and the proposed R6 on BCSI Access Management.

A couple of entities expressed concerns about a security gap – Differentiate between state protections for physical versus electronic BCSI protections.

Thank you for your comments. The SDT does not foresee a security gap. The CIP-004 standard Requirement R6 is intended to assure personnel (employee and non-employee) authorization, verification, and revocation of provisioned access to electronic or physical BCSI, whereas CIP-011 Requirement R1 covers the identification methods for the BCSI itself and the administrative or technical methods (whether electronic or physical protections) used to assure confidentiality of the BCSI. The SDT determined that, when a Responsible Entity designates material (whether physical or electronic) as BCSI, it is considered BCSI regardless of state (storage, transit, or in use) and requires protection under the information protection program.

Some entities requested the SDT to leverage the language in the current CMEP Practice Guide. State "access and use" or "obtain and use" in the requirement instead of just "use". Also, incorporate "Compliance Implementation Guidance Cloud Solutions and Encrypting BES Cyber System Information – June 2020."

Thank you for your comments. The SDT considered industry's concerns about the absence of "obtain and use" language from the CMEP Practice Guide, which currently provides alignment on a clear a two-pronged test of what constitutes access in the context of utilizing third-party solutions (e.g., cloud services) for BCSI, and agrees this is important to incorporate. As a result, the SDT mindfully mirrored this language to assure future enforceable standards are not reintroducing a gap. The SDT leveraged language from the CMEP Practice Guide to modify Requirement R6 where necessary. Please see updated modifications.

An entity expressed the wording "based on need" is not necessary within Requirement R6 Part 6.1.

Thank you for your comments. The SDT considered the wording "based on need" and determined it is imperative that the Responsible Entity have the authority to determine the business need. Removal of this language could expose entities to undue compliance risk if it is left subjective as to who determines business need. Additionally, "based on business need" is included in the current enforceable requirement. Removal of it could be perceived as materially changing or diluting the requirement that was written to achieve former FERC directives, or out of scope of the 2019-02 standard authorization request (SAR). As a result, the SDT chose to retain this language for ultimate clarity that business need is determined by the Responsible Entity.

An entity expressed that the "CIP Exceptional Circumstances" is not necessary for Requirement R6 Part 6.1.

Thank you for your comments. The SDT has identified use cases where it may not be reasonable to expect an entity to execute its authorization processes to provision BCSI access, particularly in the case of physical BCSI and physical access needs of first responders in situations of medical, safety, or other emergencies as defined by CIP Exceptional Circumstances.

An entity expressed that the measures in Requirement R6 Part 6.1 "Dated authorization records for provisioned access to BCSI based on need." The statement "based on need" is not necessary here. If it is, then be clear on the expectations that the evidence needs to document the business need.

Thank you for your comments. The SDT considered the consistency concern from the presence of "based on need" in the requirement and the way it had been used within the measure. For clarity, the SDT adjusted the bullet in the measures to provide meaningful examples of evidence for "business need".

Measures

An entity expressed concern that the CIP-004 Requirement R6 Part 6.2 measures are too detailed when referring to privileges. Many types of access to BCSI are binary, either you have it or you do not. Recommend the SDT remove the 3rd and 4th bullets in the measure so that an entity could simply verify that the access is still necessary and appropriate for their job.

Thank you for your comments. The SDT reviewed the measures and updated them by removing the third and fourth bullets.

An entity proposed using a third-party example in the measures for Requirement R6.

Thank you for your comments. The SDT wrote the measures to apply to internal or external personnel. For this reason, the SDT did not cite a specific third-party example.

CIP-011 Revisions

The SDT appreciates all comments submitted regarding the CIP-011 draft standard. The SDT reviewed each comment carefully and made respective changes where clarity or examples were needed.

Many entities expressed concern regarding CIP-011 Requirement R1 Part 1.3 and 1.4. In addition, some entities expressed that backwards compatibility would be difficult with the additional burden these subparts place on entities. Lastly, many entities requested clarity around certain wording and language. (e.g., "utilizing", consistent language with the standards authorization request (SAR), etc.)

Thank you for your comments. The SDT removed Part 1.3 and 1.4 from the CIP-011 standard which should alleviate backwards compatibility concerns and consistency with the language from the SAR.

A few entities stated that the new Requirement R1 Part 1.3 should be housed in CIP-013.

Thank you for your comments. The SDT removed Requirement R1 Part 1.3. As far as moving it to CIP-013, that is outside the scope of this project. Anyone is welcome to submit a SAR. The forms are located on the NERC Standards Resources page (link).

An entity requested the SDT be consistent between requirements and measures within CP-011 Requirement R3 Part 1.3.

Thank you for your comments. The SDT removed Requirement R3 Part 1.3 from CIP-011 and ensures that future requirements and measures are closely reviewed for consistency.

An entity requested the SDT confirm redlines posted for ballot and comment are correct.

Thank you for your comments, our apologies for the confusion. The SDT ensures the standard's redline and clean versions align for the next posting.

Measures

An entity requested the SDT be consistent throughout the opening of the measures.

Thank you for your comments. The SDT agrees with this request and modified the measures accordingly.

Some entities expressed concern that the measures for CIP-011 Requirement R1 Part 1.2 could provide audit approach confusion and requested that additional examples be provided.

Thank you for your comments. The SDT modified Requirement R1 Part 1.2 to provide clarity and additional examples.

Technical Rationale

An entity expressed that the TR for CIP-011, part 1.4, implies there would always be the state "use" in all vendor solutions. However, in this entity's experience that is not always the case, and also depends on the individual's interpretation of what "use" of BCSI means. A common example where there would not be "use" in the cloud is backup storage. (Where the data is sent already encrypted and in order to use it (aka restore) has to be called back to the customer's premises to be unencrypted.) The entity recommended the SDT remove "use", or instead change the entire paragraph to refer to the lifecycle of the data from transit to disposal.

Thank you for your comments. The SDT removed CIP-011 Requirement R1 Part 1.4 from the standard; therefore, it has been removed from the TR.

Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs)

The SDT appreciates all comments submitted regarding the VRF and VSL parts of the standards. The SDT reviewed each comment carefully and made respective changes where clarity or examples were needed.

Many entities expressed concern that the VSLs do not adequately reflect the severity of a possible violation for CIP-004 and CIP-011 modifications.

Thank you for your comments. The SDT reviewed the VSLs and modified them based on comments received.

Any entity requested that the SDT consider updating the VRF for CIP-011 Requirement R1 and Requirement R2 from a medium to a high. The basis for these reasonings are (R1) on the possible extension of BCSI to cloud providers, and the fact that there have been significantly more sophisticated, and a greater volume of, attacks against the energy industry, especially through phishing; (R2) with known foreign ownership, control, or involvement in PC reclamation and recycling, and the focus of foreign adversaries trying to gain access, cause damage, or control the US Power grid.

Thank you for your comments. The SDT reviewed the VRFs for CIP-004 and CIP-011 and determined that the standard requirements and modifications do not directly affect the grid. Therefore, the VRFs should remain a medium.

Implementation Plan

The SDT appreciates all comments submitted regarding the 18-month proposed implementation plan. The SDT reviewed each comment carefully and made respective changes where clarity or examples were needed.

18-month Implementation

In general, a majority of commenters agreed with the 18-month implementation plan. Some entities suggested 24-months as a more appropriate timeframe with the option for early adoption. It was further explained in comments that 24-months would be appropriate based on the need to revise their existing BCSI programs, an entity working with a vendor service to store, utilize, or analyze BCSI to ensure the appropriate controls have been implemented, etc.

Thank you for your comments. The SDT determined that a 24-month implementation plan would be an appropriate timeframe based on the comments received. In addition, Project 2019-02 is working closely with Project 2016-02 Modification to CIP Standards towards a seamless transition as both projects aim to combine the implementation plans later this year for NERC Board adoption. The SDT also determined that an early adoption within the implementation plan would be an appropriate modification. The SDT has modified the implementation plan to allow entities 24-months for implementation or early adoption based on discussion and agreement made with the entity's respective Region.

A couple of entities mentioned that implementation would be difficult based on ambiguity and uncertainty around respective requirements.

Thank you for your comments. The SDT encourages entities to review the provided responses to the questions regarding those respective requirements.

A couple of entities mentioned phased-in implementation should be allowed.

Thank you for your comments. The SDT believes that 24-months should allow entities ample time, and a phased-in approach is not necessary. In addition, an option for early adoption was added to the implementation plan for entities who wish to adopt the modifications sooner.

Cost-effectiveness

The SDT appreciates all comments submitted regarding cost-effectiveness among the standard modifications. The SDT reviewed each comment carefully and made respective changes where needed.

Some entities expressed concern around scope of applicability, ambiguity, unclear requirements, administrative burden, uncertainty around the word provision and how it would be used with third-party providers, etc.

Thank you for your comments. The SDT encourages entities to review the modifications made throughout the CIP-004 and CIP-011 Reliability Standards. In regards to the word provisioned, please see the TR document as it provides a thorough explanation of the word/term provision or provisioned access. This is a commonly used term among technical experts and should not cause a cost-effectiveness constraint on entities. Please also refer to the SDT's explanation under the title "Provisioned Access."