NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2019-02 BES Cyber System Information Access Management

Summary Response to Comments

Background

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

The 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 December 20, 2019 through February 3, 2020. There were 91 sets of responses, including comments from approximately 209 different people from approximately 131 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.

Question 1

The proposed revision to Requirement R1 Part 1.1 adds the requirement to identify BCSI storage locations. Do you agree that the requirement as written allows the Responsible Entity the flexibility to identify which storage locations are for BCSI? Do you agree the requirement is necessary? If you disagree with the changes made, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

Summary

A comment states the proposed changes add PCAs as applicable systems, which by definition do not contain BCSI. It seems that this addition is outside of the SAR and it would be helpful for the SDT to describe how adding this “clarifies the protections expected when utilizing third-party solutions”.

Response

Thank you for your comments. The SDT does not agree that PCAs by definition are exempt from containing BCSI. Each Registered Entity’s system and implementation is different, and there is nothing that precludes a PCA from containing BCSI. As one example, an entity may have a vulnerability scanner located within its ESP and this scanner may contain security configuration, network settings, enabled ports and services, and vulnerability status information of the BCAs. As another example, an entity may choose to implement a file server inside the ESP to store information like but not limited to ESP diagrams, response or recovery plans, system backups of conjuration files etc. which could be considered BCSI. That said, the SDT considered industry feedback and removed PCA from the Applicable Systems column.

Summary

Several commenters state that the removal of the qualifying language “with ERC” from the applicability of Medium Impact BES Cyber Systems in CIP-011-3 R1.1 as currently provided in CIP-004-6 R4.1 expands the scope of all subsequent parts of Requirements R1 and R2.

Response

Thank you for your comments. The SDT has considered these comments and has reverted the applicability to include ERC.

Summary

Several commenters believe a more effective approach would be to clearly state security objectives instead of prescriptive requirements.

Response

Thank you for your comments. The SDT agrees that objective requirements provide maximum flexibility to allow an entity to determine how to comply with the objective. The SDT was mindful to strike an appropriate balance between high level security objectives and enough detail to assure the expectations are clear.

Summary

Some commenters recommend removing “System information pertaining to” from the “Applicability” column of the Requirement Table and the applicability should be limited to BCSI.

Response

Thank you for your comments. The SDT adjusted the applicability to read BCSI as identified in Requirement R1 Part 1.1.

Summary

Some commenters believe clarification is needed in CIP-011-3 Requirement R1 Part 1.1 to identify BCSI storage locations as the requirement would create difficulty in identifying third-party storage locations or that it should be removed.

Response

Thank you for your comments. The SDT has adjusted the applicability to read BCSI as identified in Requirement R1 Part 1.1 and maintained the focus on the BCSI itself instead of storage locations. This change is fully backwards compatible and does not preclude an entity from identifying and using storage locations, while enabling entities who are ready to use of service provider technologies that are capable of applying protections to the BCSI regardless of storage location.

Summary

A comment stated that "method" should not be replaced with the term "process." A "method" for identification allows Responsible Entities to provide guidelines and criteria to their personnel to aid in identification of BCSI without requiring a pre-defined series of steps or action (e.g., a process) to be utilized by such personnel in the identification. This distinction is critical because a process can be high-level and – thereby – provide significant variability in what is identified as BCSI whereas a method provides personnel with enough guidance to provide consistency relative to BCSI identification without being overly prescriptive regarding how such identification is accomplished.

Response

Thank you for your comments. The SDT agrees with industry comments and has adjusted the requirement language to make use of the word "methods" instead of "process".

Summary

A comment stated that the SDT should create a new term "BCSI Repository"

Response

Thank you for your comments. The SDT considered industry comments to establish a new term for "BCSI Repository" because it is too prescriptive as to how an entity would have to meet the directive. For this reason, the SDT maintained the focus on the BCSI itself instead of storage locations or repositories. This change is fully backwards compatible and does not preclude an entity from identifying and using storage locations, while enabling entities who are ready to use of service provider technologies that are capable of applying protections to the BCSI regardless of storage location or repositories.

Summary

Registered entities would have difficulty proving the granting and removal of access to BCSI as contemplated in the proposed draft for CIP-004-7. As an alternative, EEI suggests using the BCSI Repository definition shown above, and revising proposed CIP-004-7 to require registered entities to prove access and removal of access to a BCSI Repository.

Response

Thank you for your comments. The SDT has revised the CIP-011-3 and CIP-004-7 requirements in order to retain backward compatibility with existing requirements where BCSI protections are applied to storage repositories. This should allow registered entities to prove access and removal of access to a BCSI Repository.

Question 2

The standard drafting team (SDT) attempted to maintain backwards compatibility with concepts of designated storage locations and access-level requirements previously contained in CIP-004-6. Do you agree that there is a minimal effort to meet this objective while providing greater clarity between BCSI and BES Cyber System (BCS) requirement obligations?

Summary

Several commenters state that Requirements related to access management should remain in CIP-004.

Response

Thank you for your comments. In response to the large number of comments received related to moving BCSI access management requirements from CIP-004 to CIP-011, the BCSI SDT has move the BCSI access management requirements back into CIP-004 in a newly created CIP-004 Requirement 6.

Summary

Switching from access controls on repositories to access controls on BCSI

Response

Thank you for your comments. The BCSI SDT has drafted a number of updates to the requirements to clarify the drafting team's intent. Primarily, the updates related to the provisioning of access in the newly created CIP-004 Requirement 6 address this concern by clarifying that it is the provisioning of an access privilege that allows ongoing access to BCSI that must be controlled, and not simply the ability to view BCSI that is made available. This clarification allows entities with access management programs focused on BCSI repositories to continue leveraging those programs, while also allowing for programs that focus on individual pieces of BCSI to implement.

Summary

Some commenters disagree with dropping the qualifying language "with ERC" from the applicability of Medium Impact BES Cyber Systems from CIP-004-6 Requirement R4 Part 4.1 when moved to CIP-011-3 Requirement R1 Part R1.3. This deletion greatly expands the scope of this requirement, and may have created a situation where Responsible Entities could be subject to multiple compliance violations based on a single action due to overlapping obligations in the CIP Standards.

Response

Thank you for your comments. The SDT recognizes that adding access management requirements for BCSI associated with facilities containing medium impact BES Cyber Systems that do not have External Routable Connectivity to the CIP-004 BCSI access management requirements is an increase in scope beyond the scope of the SAR. Therefore, this addition has been removed.

Summary

A comment states that there is not minimal effort to meet the proposed obligations due to the addition of PCAs.

Response

Thank you for your comments. The SDT recognizes that adding access management requirements for BCSI associated with Protected Cyber Assets to the CIP-004 BCSI access management requirements is an increase in scope beyond the scope of the SAR. Therefore, this addition has been removed.

Summary

Concerns with adding vendor risk assessments

Response

Thank you for your comments. The SDT made a number of updates to CIP-011 Requirement 1.3 to clarify our intent. Specifically, the assessment is not about the vendor, but instead is an assessment of the vendor's technical environment.

Summary

Some commenters noted the proposed changes may create a situation where responsible entities could be subject to multiple compliance violations based on a single action due to overlapping obligations in the CIP Standards. The proposed changes in CIP-011-3 also introduce a new complication, that of having to maintain similar access authorization, revocation and control measures as that in CIP-004-7. This could create a situation whereby a single deficiency in an entity's access management program could lead to potential non-compliance with two NERC standards at the same time.

Response

Thank you for your comments. The SDT moved the BCSI access authorization and revocation requirements from CIP-011-3 back into CIP-004-7 to eliminate the risk of potential non-compliance with two NERC standards at the same time.

Summary

A commenter does not agree with draft revisions as one of the fundamental concepts of CIP-004 Requirement R4 Part 4.1.3 that was lost in the proposed transition to CIP-011 Requirement R1 Part 1.3 is the difference between authorizing access to *BCSI storage locations,* which is a discrete and finite object that can be monitored and audited (the current CIP-004 approach), while the new CIP-011 approach is *access to BCSI* wherever and however it exists inside or outside of its storage locations (i.e. a hardcopy of a network diagram in a company truck). This fundamental change has made the requirement unmeasurable and non-auditable.

Response

Thank you for your comments. The SDT believes that this concern has been addressed through the revisions made to CIP-004-7 R6 and CIP-011 R1 Part 1.2 regarding the protection and the secure handling of BCSI, regardless of whether it is within a storage location or not.

Summary

A commenter disagrees with the addition of "disposal" to CIP-011 Requirement R1 Part 1.2.

Response

Thank you for your comments. The SDT has removed the term "disposal" from CIP-011 Requirement R1 Part 1.2.

Question 3

The SDT is attempting to expand information storage solutions or security technologies for Responsible Entities. Do you agree that this approach is reflected in the proposed requirements?

Summary

Concerns with adding vendor risk assessments

Response

Thank you for your comments. The SDT made a number of updates to CIP-011 Requirement 1.3 to clarify our intent. Specifically, the assessment is not about the vendor, but instead is an assessment of the vendor's technical environment.

Summary

A comment states it would be better to focus efforts on Requirements that do not hinder the use of other solutions while allowing for the development of access control programs by Responsible Entities that address risk posed to the industry.

Response

Thank you for your comments. The BCSI SDT has drafted a number of updates to the requirements to clarify the drafting team's intent. Primarily, the updates related to the provisioning of access in the newly created CIP-004 Requirement 6 address this concern by clarifying that it is the provisioning of an access privilege that allows ongoing access to BCSI that must be controlled, and not simply the ability to view BCSI that is made available. This clarification allows entities with access management programs focused on BCSI repositories to continue leveraging those programs, while also allowing for programs that focus on individual pieces of BCSI to be implemented

Summary

A comment states new R2 requirements are too prescriptive and cannot be prudently applied across all BCSI storage solutions and they limit the ability for the entity to manage their own compliance.

Response

Thank you for your comments. The SDT has removed R2 from the standard and incorporated it into R1.4 for clarity.

Summary

Some commenter noted the requirements as written do not clearly reflect an approach to expand information storage solutions or security technologies

Response

Thank you for your comments. The SDT thanks you for your comments. The language has been modified to allow RE's to be able to expand information storage solutions specific to third parties.

Summary

A comment suggests the team focus on the approach taken in the current NERC CMEP Guidance document in addressing the issue

Response

Thank you for your comments. The CMEP guidance has been used to directly develop the new language for controlling access to BCSI and protecting BCSI.

Question 4

The SDT is addressing, and further defining, the risk regarding potential compromise of BCSI through the inclusion of the terms "obtain" and "use" in requirement CIP-011-3, Requirement R1 Part 1.2. Do you agree that this will more accurately address the risk related to the potential compromise of BCSI versus the previous approach?

Summary

Commenters Agree with terms "obtain" and "use;" however, more explanation is needed within the requirement or guidelines. The drafting team has referred to the CMEP BCSI practice guide. We recommend defining "BCSI Access" in the NERC Glossary of Terms per the practice guide.

Response

Thank you for your comments. The SDT has taken the approach to refine the concept of access to BCSI through the ability to "obtain" and "use" within the CIP-011 Implementation Guidance, rather than the NERC Glossary of Terms.

Summary

A comment states while this approach is better than previous approaches, there is still a need for security technology vendor service providers to have access and use of BCSI.

Response

Thank you for your comments. The SDT acknowledges the potential need for vendor service providers to have the ability to "obtain" and "use" BCSI within their service model. The SDT Believes that the revisions made to CIP-011-3 R1 Parts 1.3 and 1.4 provide the Responsible Entity with the appropriate compliance framework when engaging vendor services to store, utilize, or analyze BCSI.

Question 5

The SDT is proposing to have BCSI in the "Applicability" column. Do you agree that this provides better clarity on the focus of the requirements?

Summary

Several commenters stated that the revisions expanded beyond the scope of the SAR. The commenters disagree with absence of ERC for Medium Impact BES Cyber Systems and the additions of PCAs, and want exemption for BCS, EACMS and PACS as BCSI repositories.

Response

Thank you for your comments. The SDT considered industry feedback and moved the proposed CIP-011 requirements back to the original CIP-004 requirements where Applicable Systems scopes Medium impact BES Cyber Systems with ERC, removed PCA from the Applicable Systems column, and decided to continue to scope the proposed modifications to align with the SAR objectives to focus on the BCSI.

Summary

Several commenters requested that the “Applicability” column be changed back to “Applicable Systems”. Commenters stated it creates ambiguity and inconsistency and recommends the SDT use requirement language to scope to BCSI.

Response

Thank you for your comments. The SDT removed the undefined language in favor of using the defined term BCSI to address concerns about ambiguity. The SDT adjusted the applicability to read BCSI as identified in Requirement R1 Part 1.1.

Summary

A couple of commenters noted confusion of the “applicability” as the column header with Section 4 applicability and answered in a manner that calls out a perceived issue to consider Section 4 when auditing CIP-002 citing NERC's March 1, 2019 Standards Process Manual Appendix 3A page 6 last paragraph "The only mandatory and enforceable components of a Reliability Standard are the (1) Applicability, (2) Requirements, and (3) effective dates.”

Response

Thank you for your comment. The SDT was referring to the use of the word “Applicability” in the Table Requirement Parts and the use of BCSI within that table column and not Section 4. Applicability of the CIP-011 Standard and the scope of the 2019-02 SAR. CIP-002 is not in scope for this SAR and the 2019-02 SDT cannot speak to the oversight practices for Section 4 Applicability related to CIP-002.”

Question 6

The SDT is proposing to address the security risks associated with BCSI environments, particularly owned or managed by vendors via CIP-011-3, Requirements R1, Part 1.4, and Requirement R2, Parts 2.1 and 2.2. Do you agree that these requirements will promote a better understanding of security risks involved while also providing opportunities for the Responsible Entity to address appropriate security controls?

Summary

Several commenters state that the vendor risk assessment overlaps with CIP 013 required assessment and likely belongs in CIP-013.

Response

Thank you for your comments. The SDT made a number of updates to CIP-011 Requirement 1.3 to clarify our intent. Specifically, the assessment is not about the vendor, but instead is an assessment of the vendor’s technical environment.

Summary

Some commenters note the application and language of the key control requirement is unclear in CIP-011 Requirement R2 Part 2.1.

Response

Thank you for your comments. The specific requirement related to key control has been removed.

Summary

Some commenters note the application and language of the separation of duties requirement is unclear.

Response

Thank you for your comments. The specific requirement related to the separation of duties has been removed.

Summary

Some commenters note responsible entities should have an exemption for regulators regarding these requirements.

Response

Thank you for your comments. Language has been added to the requirements to clarify that it is when a vendor's services are used that certain requirements must be met.

Summary

Several commenters state that the vendor risk assessment lacks a clear value proposition.

Response

Thank you for your comments. The SDT made a number of updates to CIP-011 Requirement 1.3 to clarify our intent. Specifically, the assessment is not about the vendor, but instead is an assessment of the vendor's technical environment. Language has been added to the requirements to clarify that it is when a vendor's services are used that certain requirements must be met.

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 should influence what if any varying controls offered by a vendor are utilized or may influence the Responsible Entity to use technical mechanisms (see CIP-0011 R2) that the Responsible Entity has more control over.

Summary

Some commenters note that these requirements may work better as guidance documents.

Response

Thank you for your comments. The SDT has made numerous modifications to ensure the requirements are clear.

Summary

Commenters voiced concern that the vendor risk assessment requires mitigation; especially since CIP-013 doesn't require mitigation.

Response

Thank you for your comments. The SDT made a number of updates to CIP-011 Requirement 1.3 to clarify our intent and the requirements for mitigation have been removed.

Summary

Some commenters noted that CIP-011 Requirement R2 could potentially be eliminated.

Response

Thank you for your comments. The SDT has clarified the intent of CIP-011 Requirement 2. This requirement is critical to ensuring the security of BCSI when utilizing a vendor's services.

Question 7

The SDT is addressing the growing demand for Responsible Entities to leverage new and future technologies such as cloud services. Do you agree that the proposed changes support this endeavor?

Summary

Some commenters note the language proposed by the SDT is too narrow and prescriptive.

Response

Thank you for your comments. The SDT has made changes to the requirements to allow for more flexibility in the use of future technologies. The requirements around key controls and separation of duties have been added to the measures and are no longer part of the requirements language.

Summary

Some commenters note this change expands the scope of these requirements beyond the original BCSI access requirements in CIP-004-6 R4 and R5

Response

Thank you for your comments. The SDT has purposefully separated BCSI access into CIP-004 and identifying and protecting BCSI in CIP-011.

Question 8

The SDT is proposing a new "key management" set of requirements. Do you agree that key management involving BCSI is integral to protecting BCSI?

Summary

Some comments note encryption should not be the only acceptable method of protecting BCSI; methods should be based on risk.

Response

Thank you for your comments. The SDT agrees with the submitters comment and has revised CIP-011-3 R1 Part 1.4 to include "one or more documented electronic technical mechanisms to protect BCSI" to allow the Responsible Entity more flexibility when considering the risk of implementation.

Summary

Some comments note the requirement is unclear if this is an electronic key or a physical key. Adding electronic key controls as prescribed by the Standard is unnecessarily burdensome for entities.

Response

The SDT has remove the specific "key management" requirement language from CIP-011-3 and replaced it with a more generic "one or more documented electronic technical mechanisms to protect BCSI" within CIP-011-3 R1 Part 1.4.

Question 9

The SDT is proposing to shift the focus of security of BCSI more towards the BCSI itself rather than physical security or "hardware" storage locations. Do you agree that this approach aids the Responsible Entity by reducing potential unneeded controls on BCS?

Summary

Several commenters stated the team should continue focusing on access controls to repositories.

Response

Thank you for your comments. The SDT has drafted a number of updates to the requirements to clarify the drafting team's intent. Primarily, the updates related to the provisioning of access in the newly created CIP-004 Requirement 6 address this concern by clarifying that it is the provisioning of an access privilege that allows ongoing access to BCSI that must be controlled, and not simply the ability to view BCSI that is made available. This clarification allows entities with access management programs focused on BCSI repositories to continue leveraging those programs, while also allowing for programs that focus on individual pieces of BCSI to be implemented.

Summary

Some commenters state that the approach as written may prevent using cloud services and may require physical protections for electronic repositories, which would preclude using cloud services.

Response

Thank you for your comments. The SDT has drafted numerous updates to clarify our intent and specifically allow Responsible Entities to leverage cloud services. Specifically, the modification to CIP-004 Requirement 6 which now focuses on the provisioning of access, and the modification to CIP-011 Requirement 1.2 which now focuses on the prevention of unauthorized access should clarify that physical access to electronic repositories is not access to BCSI. Additionally, CIP-011 Requirement 2 specifically speaks to controlling unauthorized logical access, which should also address this concern.

Summary

A commenter stated the additional controls may not have offsetting additional value to reliability and/or security.

Response

Thank you for your comments. The number and type of controls required has been streamlined and clarified.

Summary
Several commenters asserted that adding the non-ERC facilities to the access management expands the scope.

Response
Thank you for your comments. The SDT recognizes that adding access management requirements for BCSI associated with facilities containing medium impact BES Cyber Systems that do not have External Routable Connectivity to the CIP-004 BCSI access management requirements is an increase in scope beyond the scope of the SAR. Therefore, this addition has been removed.

Summary
Commenters expressed the approach isn't backwards compatible.

Response
Thank you for your comments. The BCSI SDT has drafted a number of updates to the requirements to clarify the drafting team's intent. Primarily, the updates related to the provisioning of access in the newly created CIP-004 Requirement 6 address this concern by clarifying that it is the provisioning of an access privilege that allows ongoing access to BCSI that must be controlled, and not simply the ability to view BCSI that is made available. This clarification allows entities with access management programs focused on BCSI repositories to continue leveraging those programs, while also allowing for programs that focus on individual pieces of BCSI to be implemented.

Question 10

The SDT is proposing to transfer all BCSI-related requirements from CIP-004 to CIP-011 with the understanding that this will further address differing security needs between BCSI and BCS as well as ease future standard development. Do you agree that this provides greater clarity between BCSI and BCS requirements?

Summary
Several commenter maintain that CIP-004-6 already effectively addresses access controls for BCSI stored by responsible entities

Response
Thank you for your comments. In response to the large number of comments received related to moving BCSI access management requirements from CIP-004 to CIP-011, the BCSI SDT has move the BCSI access management requirements back into CIP-004 in a newly created CIP-004 Requirement 6.

Summary
A comment recommended the SDT create Part in CIP-004 for protections where third party cloud-based services are used.

Response

Thank you for your comments. The SDT has created a new CIP-004 Requirement 6 specifically for BCSI access management and it is applicable to all BCSI access, including where third party cloud-based services are used.

Summary

A few commenters noted that it creates impossibility for compliance of individual vendor staff.

Response

Thank you for your comments. By incorporating the BCSI access concepts of the **ERO Enterprise CMEP Practice Guide***: BES Cyber System Information* into the revised CIP-011 standard language, the SDT believes that they have provided a vehicle for industry to comply with CIP-004 BCSI access requirements when using a 3rd party cloud vendor.

Question 11

The SDT increased the scope of information to be evaluated by including both Protected Cyber Assets and all Medium Impact (not just Medium Impact Assets with External Routable Connectivity). Are there any concerns regarding a Responsible Entity attempting to meet these proposed, expanded requirements?

Summary

Several commenters expressed concern of and expansion of scope to Mediums without ERC, contending BCS w/out ERC are lower risk, expansion is burdensome and not justified, and the approach does not conform to the risk-based approach that the ERO has been striving toward.

Response

Thank you for your comments. The SDT considered industry feedback and moved the proposed CIP-011 requirements back to the original CIP-004 requirements where Applicable Systems scopes Medium impact BES Cyber Systems with ERC.

Summary

Several commenters cannot support expansion to PCA. PCAs are lower risk, expansion is burdensome and not justified, and the approach does not conform to the risk-based approach that the ERO has been striving toward.

Response

Thank you for your comments. The SDT does not agree that PCAs by definition are exempt from containing BCSI. Each Registered Entity's system and implementation is different, and there is nothing that precludes a PCA from containing BCSI. As one example, an entity may have a vulnerability scanner located within its ESP and this scanner may contain security configuration, network settings, enabled ports and services, and vulnerability status information of the BCAs. As another example, an entity may choose to implement a file server inside the ESP to store information like but not limited to ESP diagrams, response or recovery plans, system backups of conjuration files etc. which could be considered BCSI. That said, the SDT considered industry feedback and removed PCA from the Applicable Systems column.

Summary

Several commenters maintain the proposed modifications are outside the scope of the SAR and do not address the SAR specifically, and should be limited to use of cloud services for BCSI and requirements to permit cloud use.

Response

Thank you for your comments. The SDT considered industry feedback and has scoped the proposed modifications to align with the SAR objectives by adjusting the requirement language to focus on "When the Responsible Entity engages vendor services to store, utilize, or analyze BCSI…"

Summary

Several commenters maintain the change in applicability to BCSI greatly expands scope to all BCSI instead of just the repositories, and is not backwards compatible with storage locations

Response

Thank you for your comments. The SDT considered industry feedback and moved forward with changing applicability to BCSI within the Requirement language. The concept that not all BCSI is in scope today is at odds with the original intent, and this adjustment brings the requirements into alignment with the security objective. The SDT has adjusted the applicability to read BCSI as identified in Requirement R1 Part 1.1, and maintained the focus on the BCSI itself instead of storage locations. This change is fully backwards compatible and does not preclude an entity from identifying and using storage locations, while enabling entities who are ready to use of service provider technologies that are capable of applying protections to the BCSI regardless of storage location.

Summary

Several commenters maintain the "System information pertaining to" language is unclear.

Response

Thank you for your comments. Thank you for your comment. The SDT removed the undefined language in favor of using the defined term BCSI. The Applicability now reads, "BCSI as identified in Requirement R1 Part 1.1"

Summary

Several commenters maintain the proposed modifications create double jeopardy concern between CIP-011 and CIP-004.

Response

Thank you for your comments. The SDT considered industry feedback and moved the proposed CIP-011 requirements back to the original CIP-004 requirements to address this concern.

Summary

Several commenters agree a PCA may contain BCSI.

Response

Thank you for your comment. The SDT appreciates your support for PCA in the Applicable Systems column. Based on industry opposition to this change, the SDT removed PCA and focused the Requirement on BCSI.

Question 12

In looking at all proposed recommendations from the SDT, are the proposed changes a cost-effective approach?

Summary

Some commenters stated that key management would result in increased costs for utilities that do not currently have key management programs in place.

Response

Thank you for your comments. The SDT has remove the specific "key management" requirement language from CIP-011-3 and replaced it with a more generic "one or more documented electronic technical mechanisms to protect BCSI" within CIP-011-3 R1 Part 1.4.

Summary

Some commenters requested to consider creating an industry standard or leveraging existing federal standards for vendors for certifications.

Response

Thank you for your comments. The SDT acknowledges the ability to leverage certification models such as The Federal Risk and Authorization Management Program (FedRAMP) would provide industry with a streamlined and cost-effective way to engage vendor services used to store, utilize, or analyze BCSI. However, this model is not feasible since NERC and Regional Entities are currently not able to rely on the work of others in lieu of direct compliance evidence. Resolving this broader topic on certification models is beyond the scope of the Project 2019-02 SAR.

Summary

Several commenters indicated that the shift from protecting repository to information level increases both cost and effort with no additional security, compliance, reliability or operational benefits.

Response

Thank you for your comments. The SDT has revised the CIP-011-3 requirements in order to retain backward compatibility with existing CIP-011-2 requirements where BCSI protections are applied to storage repositories. This should alleviate concerns where cost is an issue when protecting BCSI at the information level.

Summary

Some commenters stated that doing periodic or time-based risk assessments do not return the value especially when the risks are low and suggested entities could have the flexibility of conducting vendor risk assessment based on criteria, such as their risk management plan for high, medium and low risk posture.

Response

Thank you for your comments. The SDT believes that revisions made to CIP011-3 R1 Part 1.3 allow the entity to implement a risk assessment methodology commensurate with the type of vendor services utilized to store, utilize, or analyze BCSI.

Question 13

Do you have any other general recommendations/considerations for the drafting team?

Summary

Several commenters state that many of the proposed changes are not in the scope of the approved SAR and are too rigid.

Response

Thank you for your comments. The SDT made several updates to the CIP-011 and CIP-004 requirements and now believe that these revisions are in line with the scope of the SAR and offer more flexibility in their implementation.

Summary

Several commenters state they prefer to see goal and objective based requirements, not prescriptive.

Response

Thank you for your comments. The SDT has attempted to make the revisions to the requirements more goal and objective based.

Summary

Several commenters state the risk identification and assessment portion of the requirement overlaps with CIP-013.

Response

Thank you for your comments. The SDT worked with members from the Project 2019-03 Cyber Security Supply Chain Risks (CIP-013) drafting team to revise wording and add clarity in order to eliminate the perceived overlap between the risk assessments prescribed in the CIP-011 and CIP-013 standards.

Summary

Several commenters state that by eliminating the exclusion of Medium Impact BES Cyber Systems without External Routable Connectivity (ERC), the drafting team is exceeding the SAR.

Response

Thank you for your comments. The SDT has reinstated the Medium Impact BES Cyber Systems without External Routable Connectivity (ERC) exclusion into the CIP-004 R6 BCSI Access requirement language.

Summary

Some commenters note that Applicability should include "BES Cyber System Information stored in vendor managed electronic BCSI Repositories" (Various requirements) /SDT should draft separate requirements for cloud vs in house BCSI.

Response

Thank you for your comments. The SDT believes that it has added clarification in the CIP-011 requirements that identify those that are only applicable when the Responsible Entity uses vendor services to store, utilize, or analyze BCSI.

Summary

Commenters recommend that the scope of the standards team consider leveraging standards such as Fedramp to justify the use of cloud services.

Response

Thank you for your comments. The SDT added revised the Measures language within the CIP-011 R1.3 requirement to include Vendor certifications (i.e. Fedramp) as a potential way to confirm compliance with the CIP-011 R1.3 requirement (Risk Assessment).

Summary

CIP-011-3 R2 Part 2.1 introduces nine terms in its sub-parts 2.1.1 through 2.1.9. These nine terms are not further discussed or defined.

Response

Thank you for your comments. The SDT has deleted Requirement R2.

Summary

Several commenters state the changes to the standard do not provide any clarification regarding the definition of BCSI. Entities will need at least 24 months to achieve compliance with these new requirements. Without splitting EACMS into EACS and EAMS, the issue of third-party analysis systems is not addressed but is included in the SAR.

Response

Thank you for your comments. Revisions to the definition of BCSI within the NERC Glossary of Terms is not in the scope of the SAR. By removing some of the revisions made to CIP-004 and CIP-011 as part of the first comment/ballot posting, the SDT believes that entities can more reasonably achieve compliance within the 18-month timeframe prescribed as part of the Implementation Plan.

Summary

Commenters state that eliminate is extremely strong wording.

Response

Thank you for your comments. The word “eliminate” was removed from the revised CIP-011 requirement language.

Summary

Several commenters state it would be better to continue focusing authorization for access to storage locations and make that more robust; and Focus on Storage location BESCSI repositories.

Response

Thank you for your comments. The SDT believes that the proposed revisions to CIP-004 and CIP-011 support backward compatibility with prior versions that require controlling and authorizing access to BCSI storage locations. If an Entity wishes to continue in that manner, the revised standards would allow that.