NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Response to Comments

Project 2016-02 Modifications to CIP Standards
Virtualization | Draft 3 Posting ending April 12, 2022

Background Information

Project 2016-02 (1) addresses the Federal Energy Regulatory Commission (Commission) directives contained in Order No. 822 and (2) considers the Version 5 Transition Advisory Group (V5TAG) issues identified in the CIP V5 Issues for Standard Drafting Team Consideration (V5TAG Transfer Document).

The V5TAG, which consisted of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP Version 5 standards and to support industry's implementation activities. During the V5TAG's activities, it identified certain issues with the CIP Reliability Standards that would be better addressed by a standard drafting team (SDT) for the CIP Reliability Standards. The V5TAG developed the CIP Version 5 Transition Advisory Group Issues for Consideration document to formally recommend that the SDT address these issues and consider modifications to the standard language during the standards development process. Among other issues, the V5TAG stated "The CIP Version 5 standards comments.

Draft 3 of the Virtualization standards were posted for comment February 18 – April 12, 2022. There were 85 sets of responses, including comments from approximately 187 different people from approximately 125 companies representing 10 of the Industry.

All comments submitted can be reviewed in their original format on the project page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, you can contact Vice President of Engineering and Standards Howard Gugel (via email) or at (404) 446-9693.

The standard drafting team (SDT) considered all comments received and developed the following list of themes per question and has responded to those themes below. If you have questions, contact Senior Standards Developer, Jordan Mallory (via email) or at 404-446-2589.

Question 1

The SDT has redefined Shared Cyber Infrastructure (SCI) such that it now focuses on cyber infrastructure that shares its hardware resources among Virtual Cyber Assets (VCAs) of different impact levels only, which then subjects the SCI to additional requirements. Virtualization infrastructure that only hosts VCAs or associated VCAs of the same impact level is no longer SCI and requires no re-categorization from current state. The SDT also removed the SCI identification changes from CIP-002. The SDT believes this greatly simplifies SCI. Do you agree with the proposed change?

Q1 Comment Themes:

- Request for Implementation Guidance (IG) related to SCI

- Confusion regarding how to treat clustered versus standalone
- Clarification for where VCAs can be hosted
- SCI should not be limited to only mixed trust scenarios
- Clarification for granularity of affinity controls
- Treatment of computational workload sharing systems
- Request for further clarification of SCI
- Electronic Access Control or Monitoring Systems (EACMS) with multiple impact ratings appear to require separation
- Complexity introduced by SCI increases compliance risk
- Consensus on treatment of Virtualized assets has not been established
- Confusion if re-categorization of all assets is needed
- Treatment of Cluster versus LPARs partitions
- SCI that hosts only ancillary systems like EACMS, Physical Access Control Systems (PACS) have a different risk than ones that host BES Cyber Systems (BCS)
- High-water marking is easier than SCI, misconfigured hypervisors

  SDT Response: The SDT agrees that more scenario-based technical guidance is needed. The SDT will create more technical guidance that includes many of the scenarios suggested by the commenters.
- SCI and other forms should be included in CIP-002

  SDT Response: The SDT's SAR does not include scoping for modifying CIP-002 identification requirements to include cyber system classes that are not tied to virtualization. In draft 2, the SDT did include SCI only, but pulled that from draft 3 due to stakeholder comments. The SDT notes a new SAR has been drafted and assigned to another project that will include this issue.
- Outside of SAR
- Cyber Asset expands Scope to non-Virtual assets that was not previously included (include SAN)

  SDT Response: The SDT disagrees that the scope is expanded and that any new types of Cyber Assets are being included that were not before. The SDT is adding a new option for those Cyber Assets that support different impact ratings.
- Clarification for dormant vs non-dormant

  SDT Response: The SDT agrees and has made modifications to definitions to eliminate the use of "non-dormant", include "currently executing", and exclude "dormant images" phrasing.
- Write a separate standard for virtualization

SDT Response: The SDT is adding approximately three requirement parts to individual requirements in the CIP standards to apply to situations where multiple impact rated virtual systems may share common hardware. The SDT does not agree that a separate CIP standard is required. With the new SCI definition, the vast majority of the existing CIP requirements apply to SCI as well, therefore a SCI focused standard would require a mass duplication of existing requirements.

- Fiber channel switches or NAS configurations? How are the transport networks to be treated?

  SDT Response: The SDT intentionally decided not to include network in the SCI definition due to the overly broad inclusion that this would create, however the network elements would need to be assessed for BES Cyber Asset (BCA) inclusion as part of the CIP-002 process. For situations where the switches are critical to the function of the BCS they support, the SDT asserts that they are intended to be included in that evaluation and included as BCS. In cases where the SCI is used for systems not identified as BCA and as such not protected by an ESP, the SDT recognizes that the transport network for either fiber channel or NAS configurations could expose the storage device identified as SCI to additional surface attacks on networks outside of an identified ESP. However, the SDT asserts that these risks are minimal as the systems being hosted there would normally consist of systems like EACMS, PACS, or similar less critical systems that have traditionally already been hosted outside of the protection of an ESP. The Management Interfaces of the shared storage device identified, as SCI would need to be protected under the revised CIP-005 Requirement R1 Part 1.3 to permit only needed routable protocol communications and would assume the requirements of the systems that it supports based on the usage of SCI in the applicable systems in CIP requirements across the standards.

- Clarification on treatment of SCI in CIP-006/008/009

  SDT Response: The SDT has added SCI explicitly into several CIP-006 requirements and requirement parts. In the previous draft, it was implicit in that physical protection of VCAs entails physical protection of the hardware on which they execute, but it is now explicit in the Applicable Systems column. For CIP-008, SCI is applicable to cover the scenario where the virtualization underlay, such as the hypervisors, are being attacked or exploited but may not have reached the VCAs. For CIP-009, SCI is intentionally not applicable as entities may not necessarily plan to restore the SCI in order to restore the needed functionality of the BCS. If the entity must restore the SCI in order to restore a BCS, then the SCI should be included in the restoration plan for the BCS. The 'forensic' data preservation Requirement R1 Part 1.5 in CIP-009 does include SCI as if a VCA is compromised, preserving the data concerning the SCI could be equally beneficial in an investigation.

- More evidence required at Lows for SCI

  SDT Response: The SDT is addressing the scenario where communications may be occurring with *only* the SCI and not communicating with the VCAs it may be hosting that are part of a low impact BCS. Such communications should be subject to Section 3 of Attachment 1, as well as any TCA/RM (Section 5) connections to the SCI on which BCS execute.

Question 2

The SDT has reinstated the currently approved ESP definition and appended language to allow for zero trust models. Do you agree with the proposed change?

Q2 Comment Themes:

- Request for IG related to ESP/EAP
- Desire to implement boundary and granular access control
- The existing ESP definition is adequate
- Confusion about the use of "Cyber Asset Interface" (existing language)
- Confusion about EAP relationship to requirement language
- ESP becomes confusing without inside/outside concept

  SDT Response: The SDT agrees that more technical guidance is needed. The SDT will create more technical guidance that includes many of the scenarios suggested by the commenters.
- ESP has redundant characteristics

  SDT Response: The SDT agrees the two parts of the definition could be considered redundant as the additional language at the end could be considered a superset of the first part. However, the SDT in response to comments in previous drafts has kept the first part of the definition as-is in order to account for isolated networks that have no EAP and to insure 100% backwards compatibility. However, the additional language allows flexibility for zero-trust type architectures where access control is not based on network topology.
- Clarification for treatment of host-based firewalls
- Reinstated ESP definition but refocused on to/from BCS
- Add one or more to EAP definition

  SDT Response: The SDT agrees that more clarification is needed. The SDT has added to the EAP definition the phrase to and from “one or more” BES Cyber Systems to clarify that an EAP can control communications to a grouping of hosts. As well, the SDT added the phrase “on an EACMS” to help clarify the host-based firewall scenario.
- Zero Trust is not included in the ESP/EAP definition
- EAPs appear to be required in the second part of the ESP definition

  SDT Response: The SDT included the option for “a logical boundary defined by one or more EAPs” in the ESP definition specifically to allow for zero trust architectures. The EAP definition was also updated to include “policy enforcement points” as an option also for zero trust implementations. This allows these two definitions to work together and not prescribe that access control be only at a ‘Cyber Asset interface’ on an ESP that is only a “border surrounding a network”. As to the requirement for an EAP in the ESP definition, the SDT asserts the second half of the definition is an “or” and is a separate option for implementing an ESP. The first half of the definition, as the

currently approved language, requires no EAP and remains that way to allow for isolated networks with no external connectivity.

- EAP does not include PCA

  SDT Response: The SDT agrees and has added "and their associated PCA's" to the definition.

Question 3

The SDT modified the ERC definition from the "outside the asset containing" reference point in the previous draft back to an ESP reference point. Do you agree with the proposed change?

Q3 Comment Themes:

- Change ESP to EAP in ERC Definition

  SDT Response: The ESP is used in order to capture the grouping concept an ESP allows and to better align with the IRA definition.

- Keep existing ERC definition
- Create separate definition for ERC in Zero Trust

  SDT Response: The SDT disagrees as the ERC definition needs two updates. One to update it to allow for other forms of the remote client such as VCA, and two, to remove the "inside/outside" concept which does not align well with zero trust concepts. The SDT asserts that "from a Cyber Asset outside of its associated ESP" and "through an ESP" are essentially the same and a separate definition specifically for zero trust architectures is not necessary.

- Create definition for Zero Trust

  SDT Response: The SDT does not use the term Zero Trust within any requirements or definitions and as such asserts a definition is not necessary. Zero Trust concepts are outlined in detail elsewhere (e.g., NIST 800-207) and the SDT has taken the tact of simply removing any prescriptive language that would preclude the implementation of these concepts and replacing it with more objective language. The SDT believes this is a superior approach to defining the term and then writing prescriptive language concerning its implementation.

- Traffic between ESPs would be included in the ERC definition

  SDT Response: The SDT agrees that ERC would include external routable protocol traffic that is destined for another ESP. However, such traffic is excluded from the IRA definition. The SDT is more clearly delineating between ERC and IRA terms so they are not dependent on one another.

Question 4

The SDT has modified the IRA definition to simplify it, primarily in regards to the routable protocol to serial conversion scenario. Do you agree with the proposed change?

Q4 Comment Themes:

- IRA does not originate from an Intermediate system, add "that is not an intermediate system"

  SDT Response: The SDT agrees and has added the exclusion within the IRA definition for Intermediate Systems to avoid a recursive requirement for Intermediate Systems ("hall of mirrors").

- Consistency between lead-in on 2.1 and 2.2 (For all IRA, vs permit authorized)

SDT Response: Please see the answer to this comment under the same theme in Q7.

- IRA must initiate from external to ESP; Concerns about management systems treated as EACMS outside the ESP.

  SDT Response: The SDT asserts that the IRA definition is broad as it is defined in terms of a 'Cyber System' target inside an ESP. However, the definition is not the requirement scope and the requirement (CIP-005 R2.1) scopes IRA to only high and medium impact BCS, their associated PCAs, and any SCI that is supporting them. This is in keeping with the philosophy that glossary definitions merely define what something is, not scope of requirements nor requirements themselves. Should scoping change in the future, it can occur in the standard and its requirements, not in the glossary.

- System-to-system missing from IRA
- Clarification for user initiated (Scheduled task vs human on keys)

  SDT Response: The SDT agrees and has added the exclusion for system to system process communications that is in the current definition back into the proposed IRA definition.

- IRA required for all SCI?

  SDT Response: The SDT asserts that IRA is not required for all SCI. CIP-005 Requirement R2 Part 2.1 only applies to SCI "supporting an Applicable System in this part" and that requirement part only includes high and medium impact BCS and their associated PCAs. SCI that only supports an EACMS (that is not dual-classified as a PCA due to its location) would be an example of SCI that is not included.

- Call for CIP-015
- Too much change

  SDT Response: The SDT disagrees that such a major restructuring of the body of CIP standards is needed. The SDT is making modification to include a single scenario of the Responsible Entity converting from routable to non-routable before reaching an in-scope system. The SDT asserts this addition does not call for a major restructure or its own standard for this single scenario.

- IRA too broad; includes serial, may not be able to control outcome

  SDT Response: The SDT agrees that where the routable to non-routable conversion occurs matters. The SDT has made modifications to that bullet within the IRA definition to specify that it is in scope only when the Responsible Entity does the protocol conversion. The SDT asserts this clarifies the situation where at a substation or generator an entity may have a serial or non-routable protocol from their WAN connection they interface with, however in another entity's Control Center upstream the data is eventually converted to a routable protocol. This clarification in this bullet requires the Responsible Entity, if they perform the protocol conversion and allow IRA over it, they must implement CIP-005 R2 requirements on the routable protocol portion of the path.

- Request for IG

SDT Response: The SDT agrees that more technical guidance is needed. The SDT will create more technical guidance that includes many of the scenarios suggested by the commenters.

- Add "of a BCS" to the end of the 3rd bullet in IRA

  SDT Response: The SDT disagrees, as this would unnecessarily limit the scope of SCI that is capable of being remotely accessed with IRA. For example, SCI that is hosting only a PACS or EACMS would be excluded.

- Include definitions in the standard

  SDT Response: Approved definitions are confined to the NERC Glossary of Terms and there is no place within the standard template for definitions to be repeated within the standard.

Question 5

The SDT modified the VCA definition primarily to include the ability to host them on numerous asset types other than SCI. This allows for current state, where entities consider hypervisors as BCA, EACMS, etc. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

Q5 Comment Themes:

- Clarify excluding logical instance that are being actively remediated
- Define Active Remediation

  SDT Response: The SDT has modified the PCA and VCA definitions to clarify that the scenario intended in these exclusions is a VCA that is being actively remediated "in an environment that isolates routable connectivity from BES Cyber Systems." The SDT asserts that "Remediation VLAN" is too technically prescriptive and using VLANs may be a very common but not the only way this functionality is implemented.

- Clarify non-dormant (possibly dormant as an exclusion)

  SDT Response: The SDT agrees and has made modifications to definitions to eliminate the use of "non-dormant", include "currently executing" and exclude dormant images

- Clarify where a VCA can exist
- Clarify non-SCI cluster treatment
- Clarify hosting on other types than SCI

  SDT Response: The SDT agrees that more scenario-based technical guidance is needed. The SDT will create more technical guidance that includes many of the scenarios suggested by the commenters.

- Add containers to VCA

SDT Response: The SDT disagrees as we have considered this path and there are numerous issues with the remainder of the CIP standards should this occur. Considering packaged applications differently than other installed software on a CA or VCA, namely by considering an application equal with a CA or VCA causes a large degree of complexity and technical feasibility issues.

- IRA cannot be from a VCA because VCA is limited to a CIP type

  SDT Response: The SDT agrees and has removed "from a Cyber System" from the definition. The form the remote client takes (CA, VCA, SCI) is not material to the definition and has been removed. Thanks for the comment!

- VCA Definition: Replace "On a virtual machine" with "of a virtual machine"

  SDT Response: The SDT has made other changes to the VCA definition in response to other comments that now make "on a virtual machine" the correct form of this phrase as now it refers to a logical instance "currently executing on a virtual machine".

- TCA Clarification missing from VCA

  SDT Response: The SDT will produce more technical guidance that describes two forms of virtual TCAs and the rationale for why one form of TCA is not a required hosting platform.

Question 6

The SDT modified numerous other glossary terms. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

Q6 Comment Themes:

- Concerns about describing EAPs

  SDT Response: The SDT agrees as in zero trust methodologies there may be many EAPs involved. The SDT has added "on an EACMS" to the definition of EAP to help clarify this issue.

- Clarification for PCA definition sharing CPU and memory with hypervisor
- Clarify excluding logical instance that are being actively remediated

  SDT Response: The SDT has modified the PCA and VCA definitions to clarify that the scenario intended in these exclusions is a VCA that is being actively remediated "in an environment that isolates routable connectivity from BES Cyber Systems." The SDT asserts that "Remediation VLAN" is too technically prescriptive and using VLANs may be a very common but not the only way this functionality is implemented.

- Treat VM TCA on a TCA the same as VM TCA on other types

  SDT Response: The SDT will produce more technical guidance that describes two forms of virtual TCAs and the rationale for why one form of TCA is not a required hosting platform.

- Additional criteria in PCA adds complexity

SDT Response: The SDT agrees that the additional criteria adds complexity. However, the term PCA exists to define other cyber systems that "share" something with a BES Cyber System in such a way that they must be protected in a commensurate way, as they can be pivot points for an attack against the BCS. This 'sharing' has traditionally been only routable protocol networks; being a network peer of a BCS inside the ESP. With virtualization, another form of sharing is now available; the sharing of the execution environment – CPU and memory. Therefore, the SDT asserts the additions are necessary, however, it is not required that an entity implement in such a way that this new addition is in play.

- Definitions (such as VCA) are not clear and confusing

  SDT Response: The SDT will be producing more technical guidance for many definitions.

- Change "Acronym only " in the definition table

  SDT Response: The SDT agrees that the definition of BES Cyber System, the "Acronym only" in the proposed definition column was a note and not the definition. The SDT will fix this for the next posting.

- Management interface broader than just SCI

  SDT Response: The SDT agrees and has removed the scoping "of SCI or an EACMS" from the definition. This is in keeping with the keeping glossary terms in line with a dictionary and able to be used in other standards, while scoping and requirements are contained within requirement statements within the standards. The scoping of which Management Interfaces and what to do to them is within the CIP standards.

- ESP has been removed from the Intermediate system definition

  SDT Response: The removal of "where" an Intermediate System must be implemented has been purposefully removed from the definition and moved to an actual requirement part in CIP-005 R2. This is in line with our philosophy to put scoping and requirements in the standards and not in definitions. An entity that does not implement an Intermediate System correctly should have a requirement that is violated, not simply have no Intermediate System at all because they don't meet a requirement embedded in the definition.

- Clarification for addressing host-based firewalls

  SDT Response: See response to this theme in Question 2 above.

- Put lights out back into the Management Interface definition

  SDT Response: The SDT used this phrase in earlier drafts and received multiple comments it was too vendor-specific and to remove it with some suggestions to return to our draft 1 language. This is the path the SDT has taken in response to comments on draft 2. The SDT declines to change this back at this time.

- Add containers to VCA

  SDT Response: The SDT disagrees as we have considered this path and there are numerous issues with the remainder of the CIP standards should this occur. Considering packaged applications differently than other installed software on a CA or VCA, namely by considering an application equal with a CA or VCA causes a large degree of complexity and technical feasibility issues.

- Additional Clarification for "Cyber System"

  SDT Response: The SDT asserts that "Cyber System" is being proposed as a new definition merely as shorthand for the current 3 "forms" an in-scope object can take – CA, VCA, or SCI. This allows us to use this one term throughout the CIP standards where any form is allowed. This also allows, should more forms be needed in the future, a way to quickly add it to the standards without modifications to the entire suite.

- Put back examples of removable media, add new types

  SDT Response: The SDT declines this proposed change at this time. The SDT removed the examples as they become outdated or obsolete as technology continues to change.

- Preapprove Definitions before posting changes to standards

  SDT Response: The SDT disagrees, as many will not vote to approve terms (particularly technology terms) and definitions in a vacuum with no context as to how those definitions will be used. Also at times terms are created to match the requirements, such as IRA. Many may say that the IRA definition, in a vacuum, is too restrictive, however it is defined so that it matches scenarios where the CIP-005 R2 requirements can be met without affecting functionality or reliability of systems.

- Management Interfaces (such as vcenter) are on a separate system, may only have CIP-005 Part 1.3.

  SDT Response: The SDT asserts that some Management Interfaces for SCI are hosted on VCAs on the SCI and thus are implicitly covered in all SCI scoped requirements. However, in the scenario where the Management Interface is hosted separately on separate HW, the entity should consider in that case if that Cyber Asset is either a BCA or EACMS.

- Cyber Asset includes software, all hosted VCA are included in the definition
- When requirements are different it includes all requirements

  SDT Response: The SDT agrees and has modified the Cyber Asset definition to explicitly exclude VCAs from being software or data of the Cyber Asset. The SDT also modified the VCA definition to exclude the hardware from the VCA definition.

- Remove first bullet of Reportable Cyber Security Incident

  SDT Response: The SDT asserts the first bullet is needed for low impact systems.

- Clarifications for removing the requirement from the Intermediate System definition

SDT Response: The SDT will provide further clarification in future webinars and TR concerning the removal of requirement type language from this definition.

- Clarification for exclusions in Management Interface Definitions

  SDT Response: The SDT has agreed that the exclusions may add more confusion than clarity and has removed the exclusion. Physical interfaces such as touch panels and power switches already do not meet the 3 bullets in the definition.

- Does management Interface include Bluetooth?

  SDT Response: No, Bluetooth and other wireless technologies are transport to a Management Interface; they are not the Management Interface.

- Does not believe that VM escape is a demonstrated risk

  SDT Response: While the SDT agrees that most VM escape risks are in software and patches are typically quickly available, there are hardware-based attacks such as https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-42114 for which there are no software patches. In SCI scenarios, the criticality of BES Cyber Systems we assert warrants requiring VCA's of differing impact categorizations to not share CPU or memory simultaneously due to risks such as this CVE.

- VCAs could be considered TCAs if left less than 30 days

  SDT Response: The SDT asserts that this is not an issue specific to virtualization changes and applies equally to any physical cyber asset that does not remain connected for 30 days or more. However, the SDT notes that the TCA definition as currently approved lists TCA uses such as data transfer, vulnerability assessment, maintenance, or troubleshooting. Performing BES functions that would meet the definition of BCA, or EACMS/PACS functions would mean that system meets those definitions.

- Clarification for "prior to introduction to an ESP" regarding the PCA definition

  SDT Response: The SDT has modified the PCA and VCA definitions to clarify that the scenario intended in these exclusions is a VCA that is being actively remediated "in an environment that isolates routable connectivity from BES Cyber Systems." The SDT asserts that "Remediation VLAN" is too technically prescriptive and using VLANs may be a very common but not the only way this functionality is implemented.

- PCA definition does not have "Highest rated impact" on the 2nd bullet

  SDT Response: The SDT asserts that the only systems that have an impact rating are BES Cyber Systems. PCA's are only "associated with" a BCS that has an impact rating, they do not have one themselves.

Question 7

The SDT revised CIP-005 based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

Q7 Comment Themes:

- No ESP for SCI that only hosts EACMS

  SDT Response: The SDT agrees and has modified the applicability of CIP-005 R2.6 to exclude SCI that is not supporting a high or medium impact BCS or associated PCAs.

- Change to ESP to EAP in CIP-005 1.2

  SDT Response: The SDT asserts that EAP clarifies ESP and ESP is used in this requirement part to allow for the grouping of EAPs on an ESP such as in the case of distributed policy-based networking (i.e., zero trust).

- Consistency between lead-in on 2.1 and 2.2 (For all IRA, vs permit authorized)

  SDT Response: The SDT agrees and has made modifications to the Requirement Parts in CIP-005 R2 so that all parts begin consistently.

- Remove "authorized" and "if any" from IRA

  SDT Response: The SDT put “authorized” in the requirement part to clarify that should an attacker use some novel method to establish an unauthorized Interactive Remote Access capability not involving the entity’s Intermediate System, that would not constitute a violation of this requirement to implement an Intermediate System. The SDT does agree that the “if any” does not add any additional clarity to the requirement and has deleted that phrase.

- SCI and other forms should be included in CIP-002

  SDT Response: The SDT’s SAR does not include scoping for modifying CIP-002 identification requirements to include cyber system classes that are not tied to virtualization. In draft 2, the SDT did include SCI only, but pulled that from draft 3 due to stakeholder comments. The SDT notes a new SAR has been drafted and assigned to another project that will include this issue.

- Remove “(such as encryption)” CiP-005 R1 Part 1.4

  SDT Response: The SDT agrees and has removed the example from the requirement part and has moved it to the measures.

- Significant Effort to control Management interfaces to BCA and PCA

  SDT Response: The SDT asserts the applicability of Requirement Part R1.3 is only for Management Interfaces of SCI or EACMS and not directly to the BCA’s or PCA’s.

- Recommendation to renumber CIP-005 R1.4 to 1.6 for consistency with previous version

SDT Response: The SDT agrees and has moved the new R1.4 to the end as R1.6 to avoid any unnecessary renumbering of existing requirements within entity's programs.

- Clarification for vendor remote access and connections

SDT Response: The SDT has not made any changes to vendor remote access and refers the commenters back to the Technical Rationale documents from Project 2019-02 for explanation of those terms.

- Split SuperESP requirement back into Physical CIP-006 and Logical CIP-005
- Concern with Super ESP control in 1.4; requires physical security to fulfill a logical security control

SDT Response: The SDT asserts that these requirements have the security objective of protecting data within an ESP and allow for logical or physical options depending on the circumstance. The SDT is allowing for "across the region" as well as "across the hallway" scenarios. If some form of physical protection was required with no other option, the SDT agrees that would belong in CIP-006, but as one option among several, we assert the consolidation into CIP-005 for protecting communications within an ESP that may span PSPs belongs primarily in CIP-005.

- Clarification for handling out-of-band management

SDT Response: The SDT asserts management interfaces only apply to SCI and EACMS that enforce an ESP. Other forms of management interfaces are not addressed in our SAR.

- Don't refer to other requirement parts, spell out full applicability in each requirement part

SDT Response: The SDT asserts that would make Applicable Systems column rather unwieldy and could create maintenance issues going forward as other changes are made to the standards if these links between requirement parts are not explicit.

- Clarification for Encryption types that do not include integrity controls

SDT Response: The SDT will include a fuller explanation of the security objective within the TR.

- Move scoping for IRA from definition to requirements
- Move scoping for IRA from requirements to definition

SDT Response: The SDT asserts that moving requirements (such as where an Intermediate System must be implemented) out of the definition of what an Intermediate System is provides clarity. In the event an Intermediate System is implemented incorrectly (such as within the ESP), there should be a requirement that is violated rather than it being a matter of the Intermediate System not existing at all because what was implemented doesn't meet the full definition.

- Remove per system capability from 1.3

SDT Response: The SDT asserts that "per system capability" is needed because in some already known cases, such as many ILO cards, the ability to control incoming packets is available, but not

the ability to control its own outgoing packets. However, many other higher order systems can do both to/from and both should be implemented.

- Dialup in 1.5 does not apply to all applicable types

  SDT Response: The SDT agrees that the "with Dialup Connectivity" only applied to the BCS and not to the associated PCAs as worded and has changed the formatting of the requirement to address this concern. Thanks for your comment.

- Part 1.6 limiting to IP may restrict future technologies, prescriptive
- Scoping to routable communication leaves other protocols unprotected

  SDT Response: The SDT agrees that specifying 'Internet Protocol' is prescriptive to a degree and may limit this requirement in the future. However, it is believed that IPv4 and IPv6 are the foundational routable protocol used worldwide with no foreseeable replacement or need for replacement. The SDT chose this because this is the technology upon which practically all malicious/suspected comms detection tools are built. The SDT chose not to attempt to build an exhaustive list of the protocols and physical transport that would be excluded from such a requirement (RS-232, RS485, Fiber channel, 4-20mA current loops, etc.) and after much discussion, found that "Internet Protocol" was the most concise and long-lived scope for this requirement part.

- Change Per System Capability back to Where Technically Feasible

  SDT Response: The Per System Capability term has been used in numerous places in the CIP standards to make technical requirements conditional upon the system's capability to implement the requirement in order to avoid the TFE process overhead when a system is simply not capable of a particular requirement.

- Prescription in where MFA must occur

  SDT Response: The SDT is clarifying where MFA must occur, but not at what individual Cyber Asset or VCA it must occur as "Intermediate System" is a system level concept. The SDT asserts that the Intermediate System is the appropriate and required place for the MFA to occur, as it is not protected by the ESP and therefore this requirement strongly authenticates the user before their traffic is allowed through an ESP to a BCS. As the Intermediate System will have access to many BCS, it is appropriate to strongly authenticate the user and determine what systems they have access to before the Intermediate System allows them access to any.

- IS can be hosted on the same hypervisor as a BCA

  SDT Response: The SDT has added requirement language to requirement Part 2.6 to prevent Intermediate Systems from being hosted on Cyber Assets or SCI that also host BCS. This reduces the risk of having a BCS sharing CPU/memory with an Intermediate System whose purpose is to host a public interface.

- System-to-system missing from IRA

SDT Response: See our response to this theme under Q4.

- Clarify humans on keyboards vs scheduled tasks for IRA

  SDT Response: The SDT has added the exclusion for 'system to system process communications' back into the IRA definition.

- No minimum level of encryption is specified in CIP-005 R1 part 1.4

  SDT Response: The SDT has stated the requirement as an objective concerning confidentiality and integrity to avoid the standard having to maintain changing lists of acceptable encryption algorithms and key lengths, etc. This is a practice also used in CIP-012. The standard also cannot reference other lists by external entities that could be updated by those entities, thus changing NERC requirements outside of the SPM and its defined processes.

- Define Remediation VLAN

  SDT Response: The SDT has modified the PCA and VCA definitions to clarify that the scenario intended in these exclusions is a VCA that is being actively remediated "in an environment that isolates routable connectivity from BES Cyber Systems." The SDT asserts that "Remediation VLAN" is too technically prescriptive and using VLANs may be a very common but not the only way this functionality is implemented.

Question 8

The SDT revised CIP-007 based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

Q8 Comment Themes:

- Clarifications CPU/Memory (May be too prescriptive)
- Consider alternatives to the word "Prevent" in CIP-007 R1 Part 1.3
- Request clarifications for handling multiple impact ratings on SCI (CIP-007 R1 Part R1.3)
- No methods exist to prevent Sharing CPU/Memory on a single hypervisor

  SDT Response: The SDT asserts that in this case, the word "prevent" is the appropriate verb. In an SCI scenario, where systems of H/M/L/No impact are sharing hypervisors (e.g., within a cluster), this should only be allowed if the SCI is configured to prevent the sharing of CPU/memory resources by VCAs of different impact levels. The SDT chose to use the terms "CPU and memory resources" after considering all the various physical form factors available today for hypervisors such as HCI, frames, pods, etc. and to allow for technologies that can perform hardware partitioning within an "electronic device." The SDT has added additional examples to the Measures to help clarify this, as well as removing "in a clustered configuration" from the SCI definition as that is one, but not the only possible scenario. The SDT also modified PCA with the matching language of R1.3 "CPU or memory resources". As to methods for preventing the sharing of CPU/memory on a single hypervisor, the SDT asserts that this mainly applies today with a clustered configuration, where VCAs are sharing a group of and not a single hypervisor. In single hypervisor situations, if the SCI

cannot be configured to prevent the sharing of CPU or memory resources, then the "all-in" scenario should be used where all hosted VCAs are high-water marked through the PCA definition.

- SCI that hosts only ancillary systems like EACMS, PACS have a different risk than ones that host BCS

  SDT Response: The SDT agrees and asserts that the Applicable Systems column addresses SCI based on the risk of the systems it supports.

- TFE requires additional mitigations that are not present with Per System Capability

  SDT Response: Please see SDT response to this TFE theme under Q7.

- Clarity around System Hardening table name in CIP-007

  SDT Response: The SDT asserts that system hardening is a widely understood and long held term of art in the cyber security field. It refers to the process of configuring a system to reduce the available attack surface. A primary example of hardening is to mitigate system compromise through a discovered vulnerability in an unnecessary but still enabled (usually by default) service. Therefore, R1.1 hardens systems by only exposing to a network those services that are necessary for the system's function and disabling all others. The SDT asserts that R1 includes this, plus hardening through the disabling of unneeded physical port access, as well as using affinity/anti-affinity rules in SCI scenarios – all of which are 'system hardening' techniques to reduce available attack surface. R1 no longer deals with only 'ports and services', which was the previous title of the table.

- Define/clarify accessibility in R1.1

  SDT Response: The SDT clarifies that R1.1 applies to "routable protocol network accessibility on each Applicable System". Routable protocol access to a system is through services which open listening logical ports on a local network interface. R1.1 requires that any unneeded access over such be either disabled or prevented. This is typically implemented through disabling the service so it does not execute, or by using some other mechanism in the OS that prevents requests from arriving at the listening logical port a service has opened. "Accessibility" as used in R1.1 is at the logical, routable protocol network level and does not include physical access, logon to the physical console, code on TCA/RM, etc. The SDT chose this phrasing to make the requirement more objective oriented. The entity may choose in some situations to implement this at the "port number" level, or conversely at the "enabled service" level, or some combination as appropriate to the scenario. For example, in an SCI scenario where proprietary communications are happening in the underlay between hypervisors, having a list of necessary and enabled hypervisor services may be preferable than describing proprietary port numbering schemes of a vendor. In other situations, a list of listening ports on a network interface may be preferable. Rather than prescribe one or the other, the SDT chose to lift this to the objective level of controlling "routable protocol network accessibility".

- Disagrees with the need to document both port and service in the measures

  SDT Response: The SDT agrees and has changed the 'and' to an 'or' in the first bullet of the measure, matching the same concept in the third bullet. Thanks for the comment.

- SCI definition brings additional devices into scope

  SDT Response: The SDT asserts that any "programmable electronic devices" that meet the various functional definitions (BCA, EACMS, PACS, etc.) and all the software on them have always been in scope. The SDT is making clarifications with new terms that allow these components to be treated separately, but the SDT does not see how the scope of devices has changed. For example, a storage resource that is critical to BCS functionality, without which it cannot operate, is a part of that system.

- Request for IG around firewalls with VLANs

  SDT Response: The SDT will address such scenarios (e.g., 'firewall on a stick') in CIP-005 TR.

- Request clarity for treatment of PCAs

  SDT Response: The SDT will provide further clarity in the TR documentation for the definitions.

- Does not believe that VM escape is a demonstrated risk

  SDT Response: Please see answer to this theme under Q6.

- Provide Clarity for CIP-007 R1 Part 1.3 for Storage arrays

  SDT Response: The SDT agrees that clarity is needed for the prevention of sharing CPU or memory resources when the SCI in question is a storage array to avoid issues with, for example, caching within an array controller. The SDT has added "excluding storage resources" to this requirement.

Question 9

The SDT revised CIP-010 R1 to focus on defining change, authorizing change, and verifying that CIP-005 and CIP-007 related security controls are not affected by changes. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

Q9 Comment Themes:

- Clarification for scope of "Change"
- Clarify version changes with regards to new software
- Clarifications for custom software in CIP-010 R1 Part 1.3

  SDT Response: The SDT has added more description into CIP-010 R1.1 to further clarify the scope of changes under the change mgmt. program. The language now states "implementation of intended changes to software, or intended changes to settings that could weaken configured cyber security controls required by CIP-005 and CIP-007." We have also added the clarifier "Changes to software include the installation, removal, or update of operating system, firmware, commercial and custom software, and security patches." Several commenters pointed out that in the previous draft, it was unclear whether a user changing their password would be included (as passwords are the object of CIP-007 R5), so the SDT has clarified it is changes to *settings* that could weaken

configured cyber security controls *required* by CIP-005 and CIP-007, which would not include individual user password changes.

- Concerns about movement away from baselines

  SDT Response: The SDT considered the more policy-based and automated virtualization technologies available today and determined to change the focus of Requirement R1 towards a security objective of authorizing upcoming changes rather than mandating the maintenance of a baseline configuration. Maintaining baseline configurations remains one possible "how", but it is no longer the only prescribed "how." The phrase "baseline configuration" has been removed from CIP-010 as a result. The items found in the CIP-010-4 "baseline" are now included in the Measures column within CIP-010-5. This maintains some compatibility with current state but allows flexibility for virtualization technologies and more dynamic and automated environments. This also ensures the focus is not on documenting past changes but the authorization of current or future changes, thus making the requirement forward looking with a clearer security objective. The SDT asserts that this requirement could not remain fully backward compatible as even if the prescribed list of "trigger" items remained, as it would need to be expanded to cover additional risk items from virtualization (such as the affinity rule configuration on SCI). However, creating and maintaining baseline configurations remains a way of implementing the change management objective and remains backwards compatible from that perspective.

- CEC specific to a part or the entire requirement

  SDT Response: The SDT asserts that CEC is only included in the R1.2 requirement part concerning testing in a separate test environment. It is not included in part R1.1 as those actions can be performed after a change in an emergency. Part R1.3 on the verification of source and integrity must be done prior to the change, and the SDT asserts that should still be required in a CEC situation.

- Proposed changes are outside SAR

  SDT Response: The SDT asserts that the changes are driven by consideration of virtualization technologies and are therefore within our SAR. With concepts such as dormant VCAs, VCA's with lifetimes of hours (such as VDI instances), automated patching/AV application via remediation VLANs, and in general a more dynamic environment for the in-scope Virtual Cyber Assets, the portions of the previous requirement requiring 'backwards-looking' documentation of certain 'baseline config' attributes within 35 days of the change needed updating for the more dynamic nature of today.

- SCI definition brings additional devices into scope

  SDT Response: Please see response to this comment under Question 8.

- Implementation plan needs more than 12 months

  SDT Response: Please see response to this comment under Question 13.

Question 10

The SDT made other revisions to CIP-010 based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

Q10 Comment Themes:

- Clarification for scope of "Change" for R2

  SDT Response: The SDT agrees that the scope of change in R2 needs to match the scope in R1. The SDT has added the same language on change scope that is in R1 into R2 to accomplish this. As for more general comments on clarifying the scope of change, see the response to this comment under Q9.

- Request clarification for "prior to becoming an applicable system"

  SDT Response: The SDT used this language in CIP-010 R3.3 to accommodate remediation VLANs and the nature of VCAs that are created/built in "the production environment". As VCA's are not physical assets brought into a physical environment but are usually built in some form of isolation on the production virtualization infrastructure, the SDT looked for phrasing that could accommodate this. Since a VCA, until its instantiated and has its 'production' connectivity cannot meet the definitions of the Applicable Systems (it has no BES impact, it does not yet control access, etc.), this phrasing allows VCAs to be built and their vulnerabilities assessed before the VCA is then moved to its production connectivity and can meet the functions within the definitions of the Applicable Systems. This is the cleanest way the SDT could solve the "chicken or egg" issue of VCAs built "in the production environment."

- Consider removing new 2nd bullet from Attachment 1, Sections 1.3 and 1.4

  SDT Response: The SDT changed the "live operating system from read only media" bullets in 1.3 and 1.4 in order to accommodate broader solutions, such as "VM Player" or VM snapshots that are discarded, etc. These other types of solutions return the TCA to a known "golden image" state prior to each use and is the same objective as "live OS from read only media" without being prescriptive as to a single technical solution. As these items are in a list of options, the SDT sees no harm in including them as an option.

- Clarification for like replacements in CIP-010 in R3.3

  SDT Response: The SDT's intent is the meaning of "like replacements" is within the remainder of that bullet point, namely "of the same type of Cyber System with a configuration of the previous or other existing Cyber System." It is the same intent and objective the requirement has had in that new systems, of a type or configuration not already assessed, should be assessed before introduction into the environment.

- Request clarification for the use of Cyber System vs Applicable System

  SDT Response: The SDT asserts that in the currently approved requirement part 3.3, the standard uses the term "Cyber Asset". The SDT changed this to "Cyber System" so that if an entity was replacing a physical Cyber Asset with a VCA of the same configuration, it would not require a new

vulnerability assessment simply for the change in form. Cyber System is the term the SDT has proposed for use in situations like this where the form (CA, VCA, SCI) can vary.

- Treat VM TCA on a TCA the same as VM TCA on other types

  SDT Response: The SDT disagrees that VCA's on physical TCAs should be treated as their own distinct TCA. The SDT is addressing two different transient connection scenarios. The first scenario is a physical TCA such as a laptop. These TCA's may require older, 32-bit software and OS to connect to and configure older equipment in the field. These are often executed within VM 'player' environments on the physical TCA. The SDT asserts these packaged environments in an image file on a physical TCA should not be considered their own distinct virtual TCA. The SDT asserts that a user that is authorized to use the physical TCA should not be required to be separately authorized to execute the software they need to use on the TCA, simply because it's in an image file and executed in a VM "player" type environment on the TCA. The SDT also asserts that if the user goes to 'check out' a physical laptop to perform a job, it should not be a violation of a standard if they do not also 'check out' any VM images residing on that physical TCA's disk. That physical TCA is a 'unit' in order to perform a job and the SDT's intent is it should be treated as such. The SDT considered removing VCA's as an option for the form a TCA could take but has left it in to cover the second scenario.

  The second scenario is a more recent phenomenon where a service vendor (e.g., a pen-tester or security firm) may send an entity a VCA image (e.g., a vulnerability scanner instance) to temporarily instantiate within their virtualization environment. This VCA may only exist for a few hours and is functionally no different than the vendor bringing a physical laptop and connecting it to a physical network switch to perform the same task as a TCA. This transient VCA is not a part of the entity's CIP program and is treated as a TCA. The SDT did however add a specific exclusion for TCAs from the PCA definition so that the two definitions remain mutually exclusive. The TCA definition excluded PCA's; this makes the two mutually exclusive.

- Revert changes to keep Baselines

  SDT Response: Please see the SDT response to the baselines question under Q9.

- Clarify "version" in regard to New Software on CIP-010 R1.3

  SDT Response: The SDT agrees and has reworded the requirement to clarify that it is just not a software 'version' number change, but the installation of OS, firmware, software, or software patches. The term 'software version' is no longer in the requirement.

- Add Per System Capability for R2

  SDT Response: The SDT agrees and has added 'per system capability' to R2.

- Make Cyber System singular in R3.3;

  SDT Response: The SDT agrees and has removed the 's' so that it refers to "Cyber System".

- Changes do not appear related to virtualization

SDT Response: Please see response to comment concerning our SAR scope under Question 9.

- Request that we define Remediation VLANs

  SDT Response: See response to this issue under Q5.

- CIP-0010 R4 not scoped to associated SCI

  SDT Response: The SDT agrees and has added the word 'associated' in front of SCI in R4.

Question 11

The SDT revised CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013 mostly with conforming changes. Do you agree with the proposed changes to these Reliability Standards? If not, please provide the basis for your disagreement and an alternate proposal.

Q11 Comment Themes:

- Request clarification for CIP-003/CIP-006/CIP-009 not including SCI
- Clarification for physical protection of SCI

  SDT Response: The SDT agrees for CIP-006 that the physical protection of the SCI was implied in requiring the physical protection of the Applicable Systems. If they were VCAs, the only way to physically protect them was to protect the hardware on which they execute. However, because the VCA definition excludes the hardware, the SDT agrees it is not as clear as it could be. The SDT has added SCI to the Applicable Systems column in CIP-006 R1 and R2. For CIP-009, see response below.

- CIP-009 R1; no recovery plan required; but requires forensics for SCI

  SDT Response: The SDT, based on comments to previous drafts, removed SCI as an explicit object of a recovery plan. This is because the intent and goal of recovery is to recover the BES Cyber System functionality, which may or may not be recovered on SCI. The goal is not to recover SCI as merely SCI. Therefore, if recovering the SCI is a necessary part of recovering the BCS, then SCI should be included in the recovery plan. One example is a domain controller as an EACMS may be virtualized as a VCA on SCI. The SCI may go down and may require an extended recovery and in the meantime the entity may install Windows Server as a domain controller on a standalone server to quickly recover the functionality. However, SCI is an explicit object of the forensics requirement. In the instance that a VCA is compromised, capturing information from the SCI on which it executes is appropriate in order to investigate the compromise.

- SCI and other forms should be included in CIP-002

  SDT Response: See the response to this comment theme under Q1.

- CIP-011 R2 Part 2.1 Why is PCA a part of Part 2.1 but not R1?

  SDT Response: The SDT asserts this is existing scope not modified by this SDT under our SAR.

- Simplification of TCA mitigation bullets. Consider clarifications for new mitigations that replace Live Operating System

  SDT Response: The SDT replaced these more prescriptive bullets concerning 'live operating systems' with a more objective-based description. This was to allow for other technologies such as "VM players" that run VCA images without saving any changes made by any potential malware.

- Requests clarifications for System Capability

  SDT Response: This is a phrase that has been used in the standards since the introduction of Version 5 and this SDT is continuing to use that existing phrase. It is used to make the requirement conditional for the majority of systems for which that requirement was designed, without requiring it on every such system in existence, which does not have the capability. It allows a requirement to hit the 90-10 rule without a burdensome process.

- Treat VM TCA on a TCA the same as VM TCA on other types

  SDT Response: See answer to this issue under Q10.

- Administrative issue in CIP-008 Part 2.3

  SDT Response: The SDT agrees. This was an issue in a redline version and has been addressed by adding SCI.

- Clarify "supports any part a BES Cyber System" in CIP-003

  SDT Response: The SDT agrees after review that the "any part of" is not adding any clarity and may be confusing. The SDT has removed "any part of" phrasing.

- Vote on definitions separately

  SDT Response: See the response to the comment on "preapprove definitions" in Q6.

- "Or their successors" missing from CISA on CIP-008

  SDT Response: The SDT agrees. This was an issue in a redline version and has been addressed.

- Remove CEC CIP-006 R2.2; already covered in high level R

  SDT Response: The SDT agrees and has removed the duplicate CEC phrase in R2.2.

Question 12

The SDT has revised numerous VSL's for simplification. Do you agree with the proposed changes? If not, please provide the basis for your disagreement.

Q12 Comment Themes:

- CIP-003 Delete - "The responsible entity but failed to manage its Transient Cyber Assets"
- Per System Capability

  - CIP-004 R4.1 categories
  - CIP-005 R1.3
  - CIP-007 R4.3
- CIP-005 1.4 missing VSL

SDT Response: The SDT has reviewed these issues and has made corrections to the VSL's. Thank you for the comments. Specific to the "per system capability" comments, those are not included in any VSLs as the system capability is determined as part of the overall determination as to whether a potential violation has occurred. Once at a stage where the VSL is needed, the system capability has already been determined.

Question 13

The SDT has revised the Implementation Plan to include the Planned and Unplanned Changes provisions and to allow for early adoption. Do you agree with the proposed Implementation Plan? If not, please provide the basis for your disagreement and an alternate proposal.

Q13 Comment Themes:

- 36 month preference

SDT Response: The implementation plan and CIP-003-X from Project 2020-03 "Supply Chain Low Impact Revisions" will be combined with this SDT's package and CIP-003-Y (after successful 2016-02 ballot) and a final CIP-003-8 and integrated single implementation plan with final timeframes will be posted for comment/ballot. At this time, the SDT is not hearing a sufficient stakeholder push for more time for the virtualization changes.

- 12 Months is not enough for Changes to planned/unplanned timeframes

SDT Response: The SDT has made no changes to this longstanding language and is carrying it forward from previously and currently approved versions of the Implementation Plan.

Question 14

Please provide any additional comments for the SAR drafting team to consider, if desired.

Q14 Comment Themes:

- CIP-004 elimination of BSCI repositories

SDT Response: The elimination of BCSI "repository" language was under the Project 2019-02 SDT and was successfully balloted. This SDT is carrying their successfully balloted changes forward and has made no changes to R6 other than to add SCI to the scope.

- Clarifications for Imp plan on "Upon Commissioning"

SDT Response: The SDT has made no changes to this longstanding language and is carrying it forward from previously and currently approved versions of the Implementation Plan.

- Inconsistent use of Applicable Systems capitalization in VSL's
- Inconsistent handling of Acronyms for Definitions
- Use of BCS vs BCA inconsistent

  SDT Response: The SDT thanks you for the comments and will look for these issues as it prepares final documents for the next draft.

- SCI and other definitions are unclear about whether its dealing with on-premise virtualization or cloud

  SDT Response: The SDT is not (and it is not in our SAR) addressing cloud computing where the "programmable electronic devices" are not located on the entity's premises in one of the six CIP-002 BES asset classes listed in R1. Those six asset classes remain the scope of this version of the standards, therefore it is on-premise virtualization only.

- Implementing Affinity in SCI with multiple impact ratings is complex

  SDT Response: The SDT agrees that this is a more complex configuration option, but it has other benefits that an entity may want to take advantage of. However, the SDT notes that using SCI and affinity rules is one option and is not mandatory. The "all-in" scenario is another option without the complexity of managing affinity.

- Vote definitions separately

  SDT Response: See the response to the comment on "preapprove definitions" in Q6.

- Desire to not reuse requirement numbers (CIP-005)

  SDT Response: The SDT agrees and where possible has reordered requirement parts to better align with currently approved standards.

- No evidence of VM escape; affinity requirements not needed

  SDT Response: Please see answer to this theme in Q6.