NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Project 2016-02 Modification to CIP Standards

Comments Received Summary

There were 91 sets of responses, including comments from approximately 210 different people from approximately 133 companies representing 10 of the Industry Segments as shown in the table on the following pages.

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.

Consideration of Comments

The Project 2016-02 thanks all of industry for your time and comments.

NERC Glossary of Terms (Proposed new, modified, and retired terms)
Overall Themes concerning definitions in Q1 and SDT responses:

- Complex and difficult matrix of applicability that needs simplification
  - The SDT has made several changes in order to help simplify the “Applicable Systems” column in the standards.
- Wholesale changes are not needed, work virtualization into existing concepts with only a few virtualization specific terms needed.
  - The SDT continues to simplify and has incorporated this comment by making the “all-in scenario” possible where a virtualized infrastructure and all its components are all treated as part of its highest impact hosted BCS. This will greatly simplify and cause the least amount of changes for those using this scenario, while keeping other options open for other entities.
- Definitions are not limited in scope to virtualization only scenarios.
  - The SDT views the NERC Glossary the same as any dictionary with a purpose of simply defining what a term means, but not as a primary scoping mechanism for requirements within the standards. The glossary term and its definition should be able to be used across the NERC standards with differing scopes for different requirements, which can’t be done if the scope is part of the definition.
- The changes are not applicable to cloud, hindering NERC’s ability to move forward into cloud-based apps.

  - Enabling BES Cyber Systems to be hosted “in the cloud” on Cyber Assets outside of the entity’s physical control is not included in the scope of our current SAR. The possibility of hosting BCS in the cloud is the subject of a forthcoming NERC report on the risks and benefits of such.

- The term “cyber system” has been added in exemptions and in requirements but is undefined.
  - The SDT agrees and is providing a proposed glossary definition in the next draft and will capitalize the term where used.
- “Controlled communications” and “System hardening” added and not defined
  - For ‘controlled communications’, the SDT is using that to mean that the communications are to be controlled and the remainder of the requirement defines what that ‘control’ means: permit necessary traffic and deny all other traffic. As an example, it’s the opposite of ‘uncontrolled communications’ which would be traffic that does not pass through any type of access control (firewall as an EAP, zero trust policy mechanism, etc.). ‘System hardening’ is simply the label of a table in CIP-007 and is a common IT discipline term for reducing the attack surface of a computer system. In the next draft, one of the non-network-oriented controls will be moved to this requirement, so it will be broader than simply ports and services and ‘system hardening’ is a broader term.
- BCS definition modification is all that’s needed for virtualization
  - The SDT is incorporating the ability to have an “all-in scenario” where all the virtualization infrastructure can be included as part of an entity’s BCS in addition to allowing entities to identify it separately.
- Use the terms “virtual machine, hypervisor, virtualized host, virtualization, container” borrowed from NIST glossary
  - The SDT is using VCA and SCI in order to make some distinctions from the way others may use similar terms. For example, SCI is broader than just the software layer that virtualizes the underlay resources. It includes that, but also includes the hardware and storage controllers that share storage, as well as the management interface. We needed a more encompassing term than hypervisor alone in order to help simplify applicability. The SDT agrees with using “container” and see the response on the SCA definition comments below.
- Please clarify “Internet Protocol (IP)” as used in CIP-005 R1
  - The SDT is referring to the Internet Protocol (IP) as defined by DARPA in RFC 791 and upon which the term “TCP/IP” is based.

BCSI Definition

- “ESP names” was deleted as an example, suggest replacing with “logical isolation names”

    - The SDT deleted this because the term ESP was proposed for retirement in draft 1. In response to other stakeholder feedback, the ESP term will not be retired and this will be added back to the BCSI definition.

- The definition includes SCI, but not Management Modules or Management Interfaces.
    - The SDT agrees and has changed the nesting of these terms so that it is more all-inclusive.

Cyber Assets Definition

- Changed from plural to singular but still plural in the definition
    - The SDT agrees and will align with the currently approved definition, which is plural.
- The CA definition should not exclude SCI. SCI is a CA with a specific purpose.
    - The SDT concluded that to include SCI within the Cyber Asset definition would require a complete rewrite of that very foundational definition in a non-backward compatible way. A core issue is how the current CA definition is inclusive of all HW, SW, and data "in the device" and is problematic when the point of virtualization is to abstract and separate the 1:1 relationship of the HW from the OS/SW.

EACMS Definition

- Broaden EACMS to include and replace SCI
    - The SDT concluded that EACMS is already a very broad definition. Electronic access control is a function and as the future progresses towards Zero Trust or other architectures practically everything could become an EACMS. Additionally, the SDT is defining SCI separately so that its management interface which should be subjected to higher requirements for hypervisors hosting many BCS can be scoped to requirements without it also applying to every firewall and domain controller as an example.
- Excludes access control and monitoring to the BCS themselves, its now only to the logical isolation. Domain controllers, etc. could fall out of being EACMS if they aren't directly related to "logical isolation"
    - The SDT agrees and will make changes to reincorporate this. When changing the "of the ESP or BES Cyber Systems" to "logical isolation of the BES Cyber Systems", an unintended consequence was removing the BCS out of direct scope. Thanks for the comment and this will be addressed in draft 2.
- Should be singular, not plural (System, not Systems)
    - The SDT agrees with the point, but that is a change that would have a documentation only ripple effect through every entity's CIP program. The SDT declines to make that change at this point.

ERC Definition

- Confusing (external to what?) without ESP reference – each BCS in a rack could have ERC to its neighbor in a highly segmented network. Meant to scope the external connectivity, not within a rack.
  - The SDT agrees. With architectures such as Zero Trust shrinking ESPs to ever more granular levels, it becomes increasingly less useful as the boundary for ERC. the SDT has changed ERC to clarify that 'external' in ERC is external to the asset containing the Cyber System, which fits better with its intended scoping use as well.
- The 'from' (CA or VCA) is irrelevant. Its founded in communication, not cyber assets.
  - The SDT agrees and has removed that from the definition. It was used in the previous draft to help define what "external" meant.
- If routable protocol is being used but not through an EACMS, its not ERC.
  - While true under the previous draft definition alone, the entity would still be required to meet CIP-005 R1 which would require an EACMS to protect the applicable BCS.
- Between ERC and EACMS, one says "controlling comms" and the other says "restricting IRA". What's the difference in controlling and restricting?
  - The SDT has redefined both definitions so they use neither term.

ESP/EAP Definitions

- High degree of support for not retiring
  - The SDT is proposing to keep and redefine ESP for draft 2 in response to comments. The new proposed definition is broadened to allow for single, static perimeters around a network segment or many, dynamic "perimeters" around a session in zero trust models.
- Traditional ESPs will be used by entities for many years to come
  - The SDT agrees that the static network segment-based perimeter model has no discernable end-of-life; it will co-exist with other models such as zero trust for the foreseeable future. The SDT proposed retirement of the ESP/EAP terms in order to be more architecture agnostic, but due to feedback is reinstating both terms with broadened definitions that can accommodate other architectures.

Intermediate System Definition

- Overly broad – could potentially label other EACMS as IS. A FW restricts IRA so is any FW an IS?
  - The SDT is modifying the proposed definition to reinstate that the restriction of IRA is "to only authorized users" which was not in the previous draft. The SDT asserts this should help with clarity around this issue.
- Address IS as its own applicable system without including it in with EACMS to allow for more granular controls for IS.

  - The SDT asserts that Intermediate Systems is its own definition such that it can be called out for specific, more granular requirements in CIP-005 R2. However, it is included as an EACMS such that it is included in all the other CIP standards that apply to associated EACMS. Otherwise, Intermediate Systems would have to be added as a separate item in all other applicability columns that apply to EACMS.
- Adjust definition to recognize it could be one or more EACMS used to restrict IRA.
  - The SDT agrees and has made this modification.
- Needs the "to authorized users". Can be read that all users must be restricted from using it.
  - The SDT agrees and has made this modification.

IRA Definition

- Need to clearly distinguish between 'engineering access' and operators operating through a system.
  - The SDT agrees and has reinstated the concept of IRA being from "outside of any of the responsible entity's ESPs".
- "outside the asset" – asset is undefined, does it mean CIP-002 R1 assets? "Outside the logical isolation" – unclear
  - The SDT agrees with providing clarity around the issue of "outside of what" and has reinstated the use of ESP.
- Not limited to routable protocol, includes all serial only comms. Huge scope increase with Intermediate System implications for serial only.
  - The SDT is incorporating clarity on IP to serial conversions that allow users to interact in real time with a serial-only device (and thus not within an ESP) that is accessible via routable protocol. The SDT is reinstating the "using a routable protocol" phrase to clarify that the user is using such a protocol, but also clarifying that accessing an applicable system through a subsequent IP to serial conversion is also IRA. The SDT asserts this clarifies that serial ONLY communications are not included.
- Does not need to remove "or other remote access technology" – if no 'client' then not IRA
  - The SDT also received comments on clarifying the meaning of remote access clients or technology. The SDT proposes that the addition of "user-initiated real-time access by a person" along with "from outside of the Responsible Entity's ESPs" helps clarify the definition of IRA.
- VLANs used for logical isolation and thus IRA could occur inside of what was the ESP.
  - The SDT agrees and has reinstated the ESP within the definition.
- Every time you connect to a CIP asset in the same logical isolation area, you are doing ERC.

  - The SDT is reinstating ESP in place of logical isolation and has modified the related definitions in accordance.

Logical Isolation

- Universal support for defining this as its critical to not only CIP-005 but numerous other definitions
  - The SDT agrees. Logical isolation is indeed a foundational concept and the SDT used the term in at least four different forms which restricted us from making one definition. In response to comments, the SDT has decided to reinstate and broaden the ESP definition and reinstate its use in place of logical isolation throughout the standards.
- Need to clarify the relationship of physical isolation and logical isolation
  - See above. The SDT is reinstating the ESP term in place of logical isolation.
- Is logical isolation that is part of a system (Windows FW) the same as logical isolation of the system? If so, that makes all comms to that Cyber Asset ERC.
  - The SDT agrees and has made several changes and clarifications, including the removal of the 'logical isolation' term. We've also changed CIP-005 R1 to state "Host-based firewalls (that only protect the host on which they reside) are not a sufficient control to meet this requirement."

Management Interfaces Definition

- Include within BCS definition
  - The SDT is providing this as an option by including this definition within the SCI definition and then providing an "all-in" option where the SCI can be a part of the BCS.
- A relay control panel or on/off button could meet the definition. Is a local display 'monitoring'?
  - The SDT agrees and has added an explicit exclusion to the definition.

Management Modules Definition

- Include within the SCI or BCS definition
- Need to define 'autonomous subsystem' or otherwise clarify that an internal RAID controller that is providing management and monitoring capability is or isn't a mgt module.
- Is Wake On LAN a management module?
- Is a module part of a Cyber Asset or its own separate cyber asset?
- Should Management Modules be explicit in requiring PSPs?
  - In reference to all comments on Management Module definition, the SDT has decided to simplify and collapse Management Module and Management System into a new singular Management Interface definition and then have requirements for controlling the access to Management Interfaces.

Management Systems Definition

- Conflicts with SCI definition
- Appears to be a hypervisor, but straddles between virtual and non-virtual environments.
- Tools such as Ghost that image systems can meet this definition.
    - In reference to all comments on Management Systems definition, the SDT has decided to simplify and collapse Management Module and Management System into a new singular Management Interface definition and then have requirements for controlling the access to Management Interfaces.

PACS Definition

- Has an “or SCI” – can SCI by itself perform the PACS function?
    - The SDT agrees that normally SCI doesn’t perform the PACS function directly, but it can support the PACS function and the SDT did not want to preclude SCI in this instance from being able to be considered part of a PACS.

PCA Definition

- Makes virtualization untenable for smaller scales
    - The SDT agrees that these clarifications may require additional hypervisors in order to mitigate vulnerabilities of systems of differing impact levels sharing the same underlying hardware. The clarifications are intended to mitigate the risks of HW-based side channel or VM escape attacks from peer hosted VCAs on the same hypervisor. However, there is now an “all-in” option within CIP-002 that could help alleviate this issue.
- Not clear what is being ‘actively remediated’
    - The SDT has included this exclusion to account for remediation VLANs in which CAs or VCAs may boot in a logically isolated state, checked against policy and remediated (patched, AV updates, etc.), and then logically connected to their production network. While this automated process occurs, it may share CPU or memory with a BCS, but should not be reclassified as a PCA for that short time period of remediation.
- Is a serially connected device to a BCS now a PCA? Unclear from undefined ‘logical isolation’.
    - The SDT agrees and is reinstating a modified ESP definition.
- Is the exclusion necessary – it requires logical connection and therefore already excludes assets that are not logically connected
    - The SDT asserts the exclusion is necessary as a VCA that is being instantiated in a remediation VLAN and being checked against policy before its logically connected to a “production” network could still be sharing CPU/memory with a BCS on the same hypervisor for that brief time. The SDT asserts it should not be a PCA during the time it is being remediated simply due to this possibility.

Removable Media Definition

- How is this directly connected to a network? What's the difference in "a network not logically isolated from" and a PCA?
    - The SDT is reinstating the ESP definition and restoring the definition to its former approved state with the addition of SCI to the scope.
- Was PCA intentionally removed?
    - The SDT agrees and has reinstated PCA back into the RM definition.

Reportable CSI Definition

- The ''currently approved" doesn't match what is currently in the glossary
    - The SDT does not find any differences in the currently approved definition in our proposed document and the NERC glossary.
- Doesn't include Management Module/Management Interface (CSI definition as well)
    - The SDT agrees and has made changes in the definitions and their nesting that will include such in the next draft.

SCA Definition

- "isolated" interpreted in a network context
- Could include JRE
- Running containers can be mutable during runtime, thus fall out of the definition. Many comments on the 'immutable'
- No definition needed, use common IT terms, point CIP-010 R1 to 'application container repositories'
- Seems to allude to a software appliance/package such as a virtual FW or virtual router
    - The SDT agrees with numerous comments on the SCA definition and will not be proposing a separate definition in subsequent drafts but will instead refer to common IT terms ("application containers") in CIP-010 R1 as suggested.

SCI Definition

- Includes but conflicts with the Management System definition in the "and/or" of "initialize, deploy, and/or configure"
    - The SDT agrees and has consolidated this reference into a single instance in the "Management Interface" definition using the "and" conjunction.
- What is the scope of "share"? BCS shares resources with itself – is every physical standalone box SCI? Clarify that share is with something besides itself.

    - The SDT has modified the definition to include that SCI shares CPU and memory resources "with one or more Virtual Cyber Assets…" which should clarify this issue.

- Consider replacing SCI as high-watermarked BCA
    - The SDT has made modifications to CIP-002 to allow for such an "all-in" scenario where high-watermarked SCI can be included in a BCS, while still allowing the flexibility to identify the SCI separately. See discussion in CIP-002 Technical Rationale document.
- Virtual environments could reside within specified physical security zones thus eliminating the need for a Shared Cyber Infrastructure (SCI) definition
    - The SDT agrees that SCI must have physical security protections (per CIP-006 and CIP-003 for lows) and asserts that the SCI requires its own definitional term so that further requirements can be placed on electronic access to its management interface as one example.
- Modify CA to include entire virtualization HW infrastructure
    - The SDT concluded that would require a complete rewrite of this very foundational definition in a non-backward compatible way. A core issue is how the current CA definition is inclusive of all HW, SW, and data "in the device" and is problematic when the point of virtualization is to abstract and separate the 1:1 relationship of the HW and OS/SW.
- Modify EACMS and PACS to include underlying HW
    - The SDT has made the requested modification.
- Defines two types of objects – the hypervisor and the management system.
    - The SDT agrees it combines differing types of objects, including the shared HW itself, the hypervisor software, and the management interface as one and led to this being defined as an 'infrastructure' rather than a device. The SDT asserts this leads to more simplified applicability within the standards.
- Interpreting to mean totally separate storage array is needed if hosting any CIP asset
    - The SDT asserts a storage array that is sharing its storage resources with a BCS or associated system is within the CIP standards scope, however it does not mean that the storage array must be dedicated to only CIP systems.
- Scoping SCI 'software' - Is firmware on a server blade SCI?
    - The SDT has modified the SCI definition and asserts that the term software is included in the list of items that "share CPU and memory with one or more VCAs…" and is intended to refer to the hypervisor software.
- Doesn't include network services, but the proposed definition could include network devices
    - The SDT has purposefully not included within the SCI definition devices that share network resources, as that would include every network hub or switch as SCI, which is not the

intent. A network device, such as a switch, that is used to configure and isolate different VLAN network segments would become an EACMS, not SCI.

- Many CA's could meet SCI definition. A video card is a programmable electronic device. It shares CPU and memory with the motherboard. RAID controllers share their storage resources with the CA they are installed in.
    - The SDT asserts that both SCI and "Cyber Assets" begin with the same "programmable electronic devices" phrasing which sets them both to the same level, thus since a video card isn't considered its own Cyber Asset, it should not be SCI either. The SDT has made clarifications that SCI must share CPU and memory with one or more Virtual Cyber Assets which the SDT asserts will help with clarity.
- Could be recursive – the Management System used to configure SCI is SCI itself. Suggest splitting.
    - The SDT has removed the proposal for a Management System definition and has included that functionality in a modified "Management Interface" definition that the SDT asserts helps with clarity in this issue.

TCA Definition

- "not logically isolated" would include devices that are physically isolated
    - The SDT is reinstating the ESP definition which will help clarify this situation.

VCA Definition

- Clarify short-lived VMs. Is a VM image the VCA or the images spawned?
    - The SDT has defined Virtual Cyber Asset such that it begins with "A logical instance of…" to clarify that an executing instance is the intended target. Image files are not a VCA, but their handling is clarified in CIP-010.

NERC Reliability Standard CIP-005
Overall Themes and SDT responses:

1. Logical Isolation- Define and Clarify

   - The SDT thanks you for your many detailed comments on logical isolation. Logical isolation is indeed a foundational concept and the SDT used the term in at least four different forms which restricted us from making one definition. In response to comments, the SDT has decided to reinstate and broaden the ESP definition and reinstate its use in place of logical isolation throughout the standards.

2. EACMS and PACS- Clarity of use in requirements, - PACS or EACMS hosted on standalone hardware, relationship of virtual PACS and EACMS to SCI

   - The SDT thanks you for your comments on EACMS and PACS. In response to comments, the SDT have modified the Applicable Systems for the requirements in R1. Changes have also been made to the Requirements, and a new Requirement 1.3 created.

3. Needed and Controlled Communication- Define and Clarify

   - The SDT thanks you for your comments on needed and controlled communications. The SDT is using that to mean that the communications are to be controlled and the remainder of the requirement defines what that ‘control’ means: permit necessary traffic and deny all other traffic. As an example, it’s the opposite of ‘uncontrolled communications’ which would be traffic that does not pass through any type of access control (firewall as an EAP, zero trust policy mechanism, etc.).

4. Needed and Controlled Communication- Suggested changes - Identify needed communications and control permitted communications to and from applicable systems either individually or as a group and logically isolate all other communications, excluding time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).

   - The SDT thanks you for your comments on needed and controlled communications. The requirement has been rewritten to read “Applicable Systems connected to a network via a routable protocol must be protected by an ESP that permits only needed communications and denies all other communications, excluding time-sensitive protection or control functions between intelligent electronic devices. Host-based firewalls that only protect the host on which they reside are not a sufficient control to meet this requirement.”

5. “Define and Clarify the term Group”

   - The SDT thanks you for your comments on the wording of Requirement 1.1. In response to comments, the SDT has rewritten the requirement to read “Applicable Systems connected to a network via a routable protocol must be protected by an ESP that permits only needed communications and denies all other communications, excluding time-sensitive protection or control functions between intelligent electronic devices. Host-based firewalls that only protect the host on which they reside are not a sufficient control to meet this requirement.”

6. Clarify/simplify protocol IEC TR-61850-90-5 R-GOOSE

    - The SDT thanks you for your comments on the protocols listed in the requirement as examples. The requirement has been rewritten to remove the references and now reads “Applicable Systems connected to a network via a routable protocol must be protected by an ESP that permits only needed communications and denies all other communications, excluding time-sensitive protection or control functions between intelligent electronic devices. Host-based firewalls that only protect the host on which they reside are not a sufficient control to meet this requirement.”

7. Backwards Compatibility

    - The SDT thanks you for your comments on backwards compatibility. In response to comments, the SDT has decided to reinstate and broaden the ESP definition. The requirement has been rewritten to read “Applicable Systems connected to a network via a routable protocol must be protected by an ESP that permits only needed communications and denies all other communications, excluding time-sensitive protection or control functions between intelligent electronic devices. Host-based firewalls that only protect the host on which they reside are not a sufficient control to meet this requirement.”

8. Requirement 1.1 Overall - Changes to 1.1 not required, Keep the ESP Term

    - The SDT thanks you for your comments on R1.1. Logical isolation is indeed a foundational concept and the SDT used the term in at least four different forms which restricted us from making one definition. In response to comments, the SDT has decided to reinstate and broaden the ESP definition and reinstate its use in place of logical isolation throughout the standards.

CIP-005 Requirement R1 Part 1.2.

1. The SDT modified CIP-005 Requirement R1 Part R1.2 to establish logical isolation requirements for Management Systems, Management Interfaces, and associated SCI. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

    - Clarity on if addition of SCI results in inclusion of associated systems

        - *The SDT thanks you for your comments and has made proposed changes to the Standard to address this confusion.*

    - Clarity on applicable systems and expansion

        - *The SDT has made several changes in order to help simplify the “Applicable Systems” column in the standards.*

    - Defined Term (Management Module) excludes SCI, applicable systems includes SCI of Management Systems

        - *In reference to all comments on Management Systems definition, the SDT has decided to simplify and collapse Management Module and Management System into a new singular*

Management Interface definition and then have requirements for controlling the access to Management Interfaces.

- Need definition of Logical Isolation
  - *The SDT thanks you for your many detailed comments on logical isolation. Logical isolation is indeed a foundational concept and the SDT used the term in at least four different forms which restricted us from making one definition. In response to comments, the SDT has decided to reinstate and broaden the ESP definition and reinstate its use in place of logical isolation throughout the standards.*
- Need clarification of requirements with applicable systems of EACMS
  - *The SDT thanks you for your comments on EACMS and PACS. In response to comments, the SDT has modified the Applicable Systems for the requirements in R1. Changes have also been made to the Requirements, and a new Requirement 1.3 created.*
- Use existing definition
  - *The SDT thanks you for your comments on R1.1. Logical isolation is indeed a foundational concept and the SDT used the term in at least four different forms which restricted us from making one definition. In response to comments, the SDT has decided to reinstate and broaden the ESP definition and reinstate its use in place of logical isolation throughout the standards.*
- Need better separation for requirements between SCI and non-SCI
  - *The SDT thanks you for your comments and has made proposed changes to the Standard to address this confusion.*
- Need clarity for backward compatibility
  - *The SDT thanks you for your comments on backwards compatibility. In response to comments, the SDT has decided to reinstate and broaden the ESP definition.*
- Need better examples in Measures
  - *The SDT thanks you for your comment. The SDT has included more examples within the measures of the proposed changes.*
- Need clarity on requirements with management modules of SCI
  - *In reference to all comments on Management Systems definition, the SDT has decided to simplify and collapse Management Module and Management System into a new singular Management Interface definition and then have requirements for controlling the access to Management Interfaces.*
- Management Modules should also apply to BCAs, PACS, and EACMS that are not on the SCI. Texas RE seeks clarification on whether management modules on current applicable BCAs, PACS, EACMS that are not on SCI are applicable to the CIP Requirements and Parts in the Applicable Systems column.

  - *In reference to all comments on Management Systems definition, the SDT has decided to simplify and collapse Management Module and Management System into a new singular Management Interface definition and then have requirements for controlling the access to Management Interfaces.*

- Need to protect physical systems of virtual systems
  - *The SDT has made the requested modification.*
- Need more clarity on “controlled communication”
  - *The SDT thanks you for your comments on needed and controlled communications. The requirement has been rewritten to read “Applicable Systems connected to a network via a routable protocol must be protected by an ESP that permits only needed communications and denies all other communications, excluding time-sensitive protection or control functions between intelligent electronic devices. Host-based firewalls that only protect the host on which they reside are not a sufficient control to meet this requirement.”*

CIP-005 Requirement R1 Part 1.3.

SAR Related

- Language would require protections between two PSPs within a substation. This extends the requirement to medium impact BES Cyber Systems even non virtualized ones, which is beyond the scope of the SAR.
- Including PACS is a problem as PACS are not required to be within a PSP.
- Define "communication networks".
- Communication Networks needs to be define per Order 791 paragraph 150.
- Beyond the scope of the SAR (failed to understand we are extending a single ESP). Recommendation to revert changes.
- Should be moved back to CIP-006.

The SDT thanks you for your comments. Based on this group of comments the SDT has made modifications to the proposed language in an attempt to alleviate the concerns related to changes that are outside the scope of the SAR.

Encryption

- Suggestion to require a minimum level of encryption.
- Encryption reference should be in measures.
- Provide clarity for the "confidentiality and integrity" verbiage.
- Specific technology examples should be added to the IG as was presented in the Webinars.
- Suggestion to add "equally effective logical protection".

- Specific protocols in the requirements area should be moved to the measures area.

The SDT thanks you for your comments. Based on the comments related to encryption technologies the SDT will ensure that technology examples are added to the IG where applicable. Additionally, we will review the usage of the encryption verbiage in the requirement to evaluate if it is better placed in the measures area. Lastly, the phrase “confidentiality and integrity” is commonly understood to mean that the use of cryptographic mechanism is required to protect the data traversing between the described endpoints.

Exclusion

- Rewording of CIP-012 exclusion since Real-time Assessment and Real-time Monitoring are not clearly defined.
- Suggest changing the exclusion to "time-sensitive protection or control functions" to enable all such protocols to be included.
- Remove GOOSE exclusion and describe the general requirements of a such a protocol to enable similar protocols to be excluded.
- Exclusion should be expanded to also exclude communication to a Control Center owned by other entities.
- Exclusion should include voice communication.

The SDT thanks you for your comments. The SDT has modified the verbiage of the exclusion to remove specific protocols and utilized more generic verbiage to describe these protocols and use cases. The exclusion concerns “…data while being transmitted between Control Centers *subject to CIP-012*” and CIP-012 excludes voice communication. This requirement part, which could overlap CIP-012, includes this “subject to CIP-012” exclusion simply to avoid double jeopardy.

Physical Controls

- Confidentiality and Integrity includes physical controls, so specifically stating physical controls is redundant.
- Is physical protection enough rather than logical protection? Hardened conduits as an example.
- Add evidence of physical controls in the measures since physical controls are listed as being acceptable in the requirement.

The SDT thanks you for your comments. The phrase “confidentiality and integrity” is commonly understood to mean that the use of cryptographic mechanism is required to protect the data traversing between the described endpoints, so the SDT feels that specifically identifying physical protections is appropriate. The SDT feels that physical controls are adequate to meet this requirement assuming that those controls are properly implemented and documented per the requirement and the associated measures which have been added to the most recent draft.

Applicability

- Applicable systems uses "or" instead of "and" and is not consistent with the rest of the standard.
- Applicability is confusing.
- Applicability column is hard to read.

The SDT thanks you for your comments. The SDT agrees that the applicability column should be more easily understood and therefore it has been significantly reworked in an effort to provide additional clarity in the most recent draft.

Others

- Limits security and assumes associated devices can be compromised externally.
- Confusion about requirement when equipment is entity owned vs third party owned.
- Requires significant modifications without indicating how these changes can be accomplished in a compliant way.
- Unclear how this improves security.

The SDT thanks you for your comments. The SDT disagrees with the assertion that the draft language limits security or does not improve the security of the BES. Multiple requirements have been added or modified in an effort to better protect virtualized systems and the infrastructure that hosts the virtualized infrastructure. This has historically been an area with no associated requirements and frequently overlooked by entities. While the draft language does require significant modifications for some entities to become or remain compliant, it is up to the entity to evaluate their environment, requirements, and architecture to best construct a compliant solution.

Reliability Standard CIP-005 Requirement R2

The comments provided by industry on the posting of CIP-005-8 R2 fell into several common themes:

1. The change in the IRA definition has left the term “system to system” undefined
   - The SDT thanks you for your comments. While the approved definition of IRA stated that it is not “system to system” communications, the SDT asserts that many entities have defined “system to system communications” within their existing compliance programs. If the SDT were to define “system to system” communications, this may conflict with those entities defined definitions
2. Entities suggested that the sequence of Requirement R2 Parts 2.1 to 2.3 be changed to Parts 2.2, 2.1, 2.3.
   - The SDT thanks you for your comments. The SDT has discussed a possible change in sequence however, it concluded that this change would result in unneeded additional administrative burden on entities.

3. The IRA definition – needs to be more precise to take into account where all connections are serial based. For example, in a totally serial based system, the HMI control consoles would be considered IRA, but none of the proposed CIP-005-8 Requirement R2 controls could be applied.

    - The SDT thanks you for your comments. The SDT agrees with your comments. The SDT has updated the definition of IRA to include the qualifier "*using a routable protocol*" so as to scope out the CIP-005 Requirement R2 controls for these types of systems

4. The proposed Intermediate System definition should be "an EACMS that restrict its IRA"

    - The SDT thanks you for your comments. The SDT agrees with your comments. The SDT has updated the definition of Intermediate System to "*One or more Electronic Access Control or Monitoring Systems that are used to restrict Interactive Remote Access to only authorized users*"

5. PACS and EACMS should not be added to scope for IRA (CIP-005-8 Requirement R2 Part 2.1). EACMS also causes a "hall of mirrors" issue for Intermediate Systems (which are also EACMS)

    - The SDT thanks you for your comments. The SDT agrees some with your comments. The SDT has updated the proposed Applicable Systems of CIP-005 Requirement 2 Part 2.1 with the following additions:

        - *EACMS that enforces an ESP for the Applicable Systems in Part 1.1.*
        - *SCI identified independently supporting an Applicable System above*

      The SDT asserts that the addition of "*EACMS that enforces an ESP for the Applicable Systems in Part 1.1.*" (i.e. CIP-005-8 Requirement R1 Part 1.1) is needed to provide the appropriate level of protection for the integrity of the ESP

6. In the proposed CIP-005-8 Requirement R2 Part 2.1, the word "*Ensure*" is too absolute

    - The SDT thanks you for your comments. The SDT agrees some with your comments. The SDT has updated the wording of CIP-005 Requirement 2 Part 2.1 to "*Permit authorized IRA, if any, only through an Intermediate System*…."

7. For the proposed CIP-005-8 Requirement R2 Part 2.6, why is affinity needed for virtualized Intermediate Systems?

    - The SDT thanks you for your comments. The SDT asserts that some entities have architected their Intermediate Systems to allow remote users to connect directly from the Internet. The SDT asserts that this type of architecture dramatically increases the cyber-attack surface area beyond that which would be normally associated with an internal corporate / business cyber system. As a result, the SDT asserts that the affinity requirement for Intermediate Systems is needed to cover this type of situation.

8. In the proposed IRA definition, what is a "remote access client"?

    - The SDT thanks you for your comments. The SDT has updated the proposed definition of IRA to "*User-initiated real-time access by a person…*" to eliminate this confusion.

9. When and where is encryption required for IRA?

    - The SDT thanks you for your comments. The SDT asserts that the proposed wording of CIP-005-8 Requirement R2 Part 2.2 is clear enough such that these controls are only required between the client and the Intermediate System.

NERC Reliability Standard CIP-007

The comments provided by industry on the posting of CIP-007-7 fell into several common themes:

1. The clarity, and value of requirement language was questioned, as well as the security concern over dynamic port allocations and over broad port ranges, with the shift from logical network accessible ports to network accessible services.

    - The SDT thanks you for your comments and is working to modify the ports and services requirements to address multiple clarity and security concerns present in the original wording.

2. There were several comments that indicated that a disparity exists with respect to how the term “system hardening” is used throughout CIP-007-7.

    - The SDT thanks you for your comments, however the team feels that the term is consistently used throughout CIP-007-7 and does not intend to modify the use of the term. The SDT will likely incorporate additional discussion of system hardening in the forthcoming Implementation Guidance.

3. There were several comments that indicated that many of the changes were not backwards compatible, especially with respect to SCI.

    - The SDT thanks you for your comments and has identified a path forward that will allow entities to include SCI within a BCS, EACMS or PACS, or identify the SCI independently. The entity benefit to the former is simplicity, where Requirement Applicability is modified to allow entities to treat their SCI as just a part of a BCS, and therefor increasing the backwards compatibility of the proposed language. The entity benefit of the option to identify SCI independently is the increased flexibility in hosting systems of differing impact on one SCI.

NERC Reliability Standard CIP-010

The comments provided by industry on the posting of CIP-010-5 fell into several common themes:

1. Many of the comments dealt with the removal of the “baseline” from the requirement language in CIP-010 R1. Some suggested that there was a security concern in doing so, others simply asked for additional clarity in the change.

    - The SDT thanks you for your comments and has chosen to include a description of the use of the “baseline” concept within the measures of CIP-010. In taking this step the SDT hopes to provide the requested clarity. The SDT has chosen to respond to the comments suggesting a security concern over the authorization of the software that is initially installed on a system, by stating that this is not a requirement in the current version of CIP-010. The authorization required by CIP-010-4 is to changes to the current baseline, and therefore the initial authorization of the baseline is not a required step. While this is a positive security control, it is not required by CIP-010.

2. Many comments suggested that the SCI entries in the Applicability column were extremely confusing and difficult to understand.

    - The SDT thanks you for your comments, and agrees with the stated concerns, and has addressed this concern by simplifying both the Management related definitions down to one, and the SCI Applicability column insertions. These SCI Applicability column insertions as much simpler and the SDT hopes easier to understand by referring to the other Applicable Systems.

3. There were also many comments that provided feedback on unintended scope changes found within the proposed Requirement language.

    - The SDT thanks you for your feedback and has modified the Requirement language to reinstate the scope that was originally found within the language wherever possible. There still remain some aspects of the Standard that are not backwards compatible with respect to scope, but the SDT believes to have resolved each case of unintended scope change.

4. Many commenters suggested that the inclusion of Self-Contained Application (SCA) as a defined term, and to have is then appear within the scope of CIP-010 was unnecessary, as these should already have been included.

    - The SDT thanks you for your comments, and has removed the SCA as a defined term, and resolved to use the common term “application container” in its place. The reason the SDT chose to continue to include this term is to reinforce the concept that this is truly just software, and not to be construed as a Virtual Cyber Asset.

5. There were a number of commenters that suggested that inclusion of “images used to derive operating systems or firmware” in the Requirement language of CIP-010 is unnecessary since they should have been included already.

    - The SDT thanks you for your comments and has included the addition of “images used to derive operating systems or firmware” found in Requirement Part 1.1.1 to account for the concept of virtualized systems based on a “parent image.” These images may be updated separately from a derived virtual machine and become active as soon as the virtual machine is rebooted. In this case, changes to this parent image must follow the management requirements found in Requirement R1. The SDT asserts that while it may be included by implication, the inclusion provides needed clarity and focus around this scenario.

6. There were several comments that indicated a challenge with the shift to service, from ports, with respect to SCI, and that did not coincide with the shift in CIP-007.

    - The SDT has made changes to move SCI only Requirement language to a separate sub-part of R1, and coordinate ports and services language with the updated CIP-007 R1 Part 1.1 Requirement language.

7. There were also comments that indicated that the inclusion of SCI only requirement language within CIP-010 R1 Part 1.1 along with all the other portions caused confusion and created unintended challenges.

   - The SDT thanks you for your comments and has chosen move SCI only Requirement language to a new sub-part of CIP-010 R1.

8. There were also a few comments that indicated that the new CIP-010 R1 Part 1.1. change authorization requirement did not include a timing element.

   - The SDT thanks you for your comments and has chosen not to alter the Requirement language to include the timing element. This is consistent with the current version of CIP-010-4 and offers the most flexibility with respect to how an entity should implement this requirement. Additionally, this can be used to avoid the need for a CIP Exceptional Circumstance exception to the requirement, if an entity builds in an emergency change authorization concept to expedite these changes.

NERC Reliability Standards with Conforming Changes

1. Some commenters expressed concern regarding the conforming changes to the language for Exemptions 4.2.3.2 and 4.2.3.3 regarding cyber systems

   - The SDT agrees with your comments. The SDT has added a definition for Cyber System

2. Some commenters expressed concern regarding some of the conforming changes to CIP-002. They appear to be missing Management Modules. In addition, SCI is missing from Attachment 1, Criteria 2.1.

   - The SDT has modified the proposed definition of “Management Interface” so as to incorporate “Management Modules” into “SCI”. The SDT has also modified Attachment 1, Criterion 2.1 to incorporate SCI

3. Some commenters requested the SDT develop additional Technical Rationale.

   - The SDT updated the TR where necessary and encourages review of the updates.

4. Some commenters requested the SDT consider the addition of CEC in other respective areas of the CIP Standards.

   - The SDT thanks you for your comment and the current CEC changes are within the scope of our SAR. Overall changes to the CEC concept are outside the scope at this time.

Implementation Plan

There were some commenters who supported the 24 month implementation plan; however, some entities requested between 30 and 48 months. In addition, there were some requests for a phased-in/staggered implementation option.

- The SDT thanks you for your comments and has chosen not to change the implementation plan. 24-months should be sufficient time for the type of changes needed before becoming compliant. In addition, the SDT choose not to add a phased-in/staggered approach as the early adoption or two years should suffice.

Additional Comments Received

1. Some commenters asked the SDT to be consistent across the applicability columns.
    - The SDT focused on this during their draft 2 changes and the applicability columns are in a consistent state across the standards where applicable.
2. Some commenters expressed that more requirements were focused on virtualized assets versus physical assets.
    - The SDT charge for this project is to make modifications to clarify virtualized environments within CIP. There are additional requirements for virtualized systems due to the risks inherent in sharing underlying infrastructure (SCI) and access to the management interfaces that configure and control the SCI. These risks are not present with dedicated physical assets.
3. Some commenters expressed that virtualized environments can already be used and are not needed.
    - The SDT agrees that virtualization is allowed under the current CIP standards. The charge of this project is to provide additional clarity and to address risks from sharing cyber infrastructure. The SDT in draft 2 is including an “All-In” option which will preserve current state to a large degree for those with a dedicated virtualized environment where all parts are considered part of the BCS, but is allowing flexibility such that this is not the one prescribed way to treat SCI.
4. Some commenters expressed concern that the changes do not allow full backwards compatibility.
    - The SDT asserts that all modifications being made are being made with backwards compatibility in mind. For non-virtualized systems, backwards compatibility is being maintained with a few exceptions that are driven by security risks, such as protecting access to the Management Interfaces of EACMS that enforce ESPs
5. Some commenters expressed that there were too many modifications made to the standards.
    - The SDT thanks entities for this feedback and has reinstated terms such as ESP that have allowed draft 2 to revert a number of the draft 1 changes back to currently approved language. Note that the redlines posted with Draft 2 are against Draft 1 and thus do not reflect the degree of change from currently approved standards.
6. Some commenters expressed “change fatigue” and that the changes are administrative in nature.

- The SDT can’t address concerns with the amount of version revisions by various SDTs. The SDT assumes that the comment on ‘administrative changes’ is due to the need to redefine all SCI in CIP-002 and treat is separately from the BCS it supports. The SDT has added flexibility in Draft 2 that allows for an “All-in” scenario that can help alleviate this concern.

7. Some commenters requested the GTB be inserted back into the standards.
    - The SDT thanks you for your comments; however, this is a NERC initiative across all standards and the GTB has been incorporated into technical rationale and implementation guidance respectively. Documents will be able to be accessed via the project page.
8. Some commenters acknowledged inconsistent format across all CIP Standards.
    - The SDT thanks you for your comments and has reviewed the standards to ensure format consistency across the CIP Standards.
9. Some commenters question the simultaneous posting between virtualization and BCSI projects.
    - The BCSI project has concluded and passed final ballot in June 2021. Draft 2 of the virtualization changes have been made to the final BCSI documents and now include those changes. BCSI was assigned a –X version number and virtualization a –Y version number. This allowed both projects to conclude a comment and ballot period during the same time and will assign correct version numbering upon completion of the projects.
10. Some commenters requested the SDT add identification of all systems to CIP-002.
    - The SDT reviewed and determined that adding identification of all systems (EACMS, PACS, PCA, etc.) is outside the scope of the SAR of this project.
11. Some commenters expressed concern regarding crossover from the standard modifications and the CMEP Practice Guides.
    - The SDT reviewed the respective CMEP practice guides. In addition, discussion was held with NERC compliance and determined that practice guides are used for currently enforceable standards and are reviewed as modified standards are completed and approved.