NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Virtualization and Future Technologies: Case for Change White Paper Consideration of Comments

Project 2016-02 Modifications to CIP Standards

The Project 2016-02 SDT (SDT) developed the "Virtualization and Future Technologies Case for Change" White paper to explain the need to change the cyber security CIP Reliability Standards. This white paper has not been approved or endorsed by NERC and solely includes the views of the SDT.

Recognizing the continuing growth in technology innovation, many entities in the Electricity Sector have implemented virtualization as part of their CIP programs. Many of these same entities, however, have implemented this new technology without taking full advantage of virtualization's advanced capabilities. There are several reasons for this from the constraints of the current CIP architecture to the ongoing ambiguity around how new virtualization technology applies to CIP compliance. Some of those who are implementing virtualization are experiencing a great deal of uncertainty and difficulty around developing implementation strategies that will support compliance and achieve greater reliability and security. The SDT was assigned the task to address the technological innovation in virtualization within the CIP standards.

The SDT's purpose of incorporating the virtualization concept into the CIP standards is not to merely augment the current standards. The SDT's intent is to better position the CIP standards to be applicable to any future technological innovation. Leveraging the abstraction that virtualization provides will allow the industry to more readily adopt new technology and increase security posture. This paper presents the SDT's case for change to the NERC CIP standards that is needed to allow for the innovative security techniques and new concepts brought about by virtualization.

The SDT thanks the industry for its time and attention to these matters and the resulting comments. The more popular, overall themes from the comments received have been captured and considered in this report, in order to progress towards a formal posting.

Overall Themes

- **Commenters were unclear as to how the SAN would be classified and treated.** The Standards Drafting Team thanks you for your comment. The SDT contends that due to nature of the overall configuration of traditional SANs (i.e. non-IP transport protocols, data de-duplication, volume spanning across multiple drives, etc.), that this is better addressed as part of a future change to CIP-011. The SDT is considering how to address CIP-005 issues with non-IP based protocols typically used in SANs. Please refer to the forthcoming CIP-005-7 Technical Rationale for Requirement R1.5.

- **Commenters were concerned regarding double jeopardy if both the virtual machine and the host are cyber assets.** The Standards Drafting Team thanks you for your comment. The SDT contends that the physical equipment that is hosting Virtual Cyber Assets should fall within the proposed new Shared Common Infrastructure (SCI) definition. The SDT will consider this situation while drafting the next version of the standard.
- **Commenters questioned if programmable electronic devices exclude a virtual machine.** The SDT thanks you for your comment. The NERC Glossary definition of Cyber Asset has a direct tie to the hardware on which it relied. This affected the definitions of the "Applicable Systems" terms such as BES Cyber Systems (BCS), EACS, PACS, and Protected Cyber Assets (PCAs). Because the Reliability Standard is applicable to the systems, the control for the Cyber Assets also applies to the hardware. This tie to hardware implies a singular one BCA, EACS, PACS or PCA per individual hardware system. This singularity is what virtualization intentionally breaks to increase reliability, and resiliency.

  The proposed NERC Glossary definition of Virtual Cyber Asset (VCA) and ESZ allow the tie between a specific piece of hardware and the related applicable systems to no longer be singularly defined. The VCA definition references a newly defined term, Shared Cyber Infrastructure (SCI) that does not include hardware. The definition of VCA is not inclusive of hardware, and the EACS, PACS and PCA definitions have been updated to allow for VCA versions. With the addition of SCI and revisions to the "Applicable Systems", there can be one or more virtualized instances of a BCA, EACS, PACS or PCA that reside on a single SCI.
- **Commenters were concerned with cloud services.** The SDT thanks you for your comment. At this time, the changes that the SDT have proposed are intended to better futureproof the standards for the use of the same virtualization technologies that cloud providers use, but for in-house (on-premise) system. While this sets the stage for facilitating future considerations such as the use of cloud providers, the SDT is not addressing the hosting of BES Cyber Systems with off-premise cloud providers at this time.

  The SDT notes that at some later date, it will be making conforming changes in the CIP Standards in collaboration with the NERC Project 2019-02 BES Cyber System Information Access Management SDT.
- **Commenters were concerned about the technological advances that are occurring and the desire for standards to evolve to accommodate these developments.** The SDT thanks you for your comment. At this time, the changes that the SDT have proposed are intended to better futureproof the standard to reduce the number of changes required as technology evolves. The SDT contends that while futureproofing the standards for future technological changes is desirable, this must be balanced against the need for backward compatibility to exist where possible.
- **Commenters expressed that regulatory standards should not preclude the use of resources that are generally available and meet security objectives.** The SDT thanks you for your comment. Project 2016-02 SDT was assigned the task to address the technological innovation in virtualization within the CIP standards. The SDT's purpose of incorporating the virtualization concept into the CIP standards is not to merely augment the current standards. The SDT's intent is to better position the CIP standards to be applicable to any future technological innovation. The SDT agrees that the standards should be

flexible to meet security objectives with currently available resources and not prescribe technologies or architectures.

- **Commenters expressed that changes should apply to both physical and virtual devices.** The SDT thanks you for your comment. At this time, the changes that the SDT have proposed are intended to better futureproof the standard to reduce the number of changes required as technology evolves. The SDT contends that while futureproofing the standards for technological evolution is desirable, this must be balanced against the need for backward compatibility to exist where possible. This need for backwards compatibility may limit the number proposed changes possible to physical devices.
- **Commenters were concerned with problems related to multi-role devices not specific to virtual devices.** The SDT thanks you for your comment. The SDT intends to address of the possibility that Cyber Assets may fall within multiple classifications (i.e. simultaneously be both SCI and PCA) and as well as how this should be addressed within the forthcoming Technical Rationale document. Please refer to the forthcoming CIP-005-7 Technical Rationale.
- **Commenters expressed concern with the overlap of CIP-012 and the "Super ESP."** The SDT thanks you for your comment. This potential overlap was resolved with the exclusion language proposed within CIP-005-7 R1.3.
- **Commenters expressed that "per system capability" should be added to the management plane isolation requirement.** The SDT thanks you for your comment. The SDT intends to address the "per system capability" scoping mechanism vs. requiring Technical Feasibility Exceptions where this is appropriate.
- **Commenters were concerned with the potential of continuing the EAP concept within the CIP standards and the potential of a one-to-one definition of EAP to Cyber Asset.** The SDT thanks you for your comment. The SDT has proposed retiring the EAP definition. With the move to an objective based requirement in CIP-005 and the need to not prescribe a cyber asset interface, an electronic access point, on a network boundary as the only model for addressing network access control, the term EAP is no longer used within the standard and is proposed to be retired. Entities are free to continue to use the term in their internal documentation to maintain backwards compatibility.
- **Commenters expressed that SCI needs to be better defined to highlight the differences between it and regular assets.** The SDT thanks you for your comment. The SDT has proposed the following definition for SCI: "Programmable electronic devices whose compute, storage (including network transport), or network resources are shared with one or more Virtual Cyber Assets or that perform logical isolation for an ESZ or ESP. This includes its management systems." The SDT's intent with this definition was to distinguish SCI from regular assets.
- **Commenters requested to address mixed use environments.** The SDT thanks you for your comments. The SDT intends to address the use of "mixed trust" through two methods. Please refer to the forthcoming Technical Rationale.

  The use of "affinity" within the Shared Common Infrastructure (SCI) will ensure that only Virtual Cyber Assets of the same "trust" level will be allowed to share CPU and system memory. This is to prevent the possibility that vulnerability within a Virtual Cyber Asset of lower trust level could be exploited to gain control of another Virtual Cyber Asset of higher trust level running on the same hypervisor within the SCI.

The high water marking of security requirements (i.e. “equalizing” or “high water marking” the R’s) results in some Virtual Cyber Assets now sharing equal trust levels. This allows these Virtual Cyber Assets to share the same CPU and system memory with the supporting SCI.

- **Commenters were concerned about the future consistent auditing approach of these modifications.** The SDT thanks you for your comment. The SDT has previously worked with NERC and the Regional Entity auditors on our approach and plan to continue working with the Monitoring and Enforcement teams as development of the standards progress.
- **Commenters expressed confusion over the options and the hypervisor isolation.** The SDT appreciates the support on the concepts of Virtual Cyber Assets, Virtual Storage and Remediation VLANs. In the Case for Change white paper, the SDT did not intend to imply that distributed firewalls, zero trust models and management plane isolation were not possible with the current standards. The intent was to show that because of how the current standards are written, using these technologies is not encouraged, and in fact could be discouraging these methods, with the amount of administrative overhead they could entail.

  The SDT has considered the comments on Management Plane Isolation and agrees. This is reflected in our proposed R1 for CIP-005.
- **Commenters expressed the desire to create two sets of standards (physical and virtual).** The SDT thanks you for your comment. The SDT asserts that the virtual vs physical assets perform the same function and it is difficult to ascertain which standard to apply to each asset as most entities use a hybrid configuration. The SDT is incorporating new definitions and objectives based requirements to address the differences between the two types. Requiring security objectives to be met should decrease the need to be prescriptive on the difference between physical and virtual systems.
- **Commenters expressed that the CIP standards already allow for virtualization.** The SDT thanks you for your comments. The SDT recognizes that some entities have already made use of Virtualization under the existing CIP Standards or contend that the existing CIP standards do not require any changes to accommodate Virtualization.

  The SDT contends that by moving the CIP standards forward from their existing “technical requirement” basis to a more “security objective” basis will result in better futureproofing as technology evolves.

  While many of the technical concepts utilized by virtualization currently exists and could be retrofitted within the existing CIP Standards, the move towards “policy based” security controls will better fit within the “security objective” based framework of CIP standards.
- **Commenters expressed a desire to include more compliance examples and clarity to better evaluate proposed changes.** The SDT intends to produce more detailed documentation in both the forthcoming Technical Rational and Implementation Guidance to assist entities to evaluate the proposed changes.

- **Commenters expressed the need to allow for backward compatibility.** The SDT thanks you for your comments. The SDT recognizes the substantial investment that entities have made in their programs to meet the existing CIP requirements. As such, the SDT has prioritized ensuring that backwards compatibility exists for current physical infrastructure installations.

  In some cases, full backwards is not possible as the SDT is also tasked with providing clarity in situations which were not envisioned in earlier versions of the CIP Standards. The forthcoming Technical Rationale document is intended to highlight where such situations exist.

- **Commenters expressed the need for clarity on "Super ESPs."** The SDT thanks you for your comments. The SDT recognizes that entities need clarity on how situations involving how "Super ESPs" should be handled. Please refer to the forthcoming Technical Rationale document in the section entitled, "Requirement R1 Part 1.3". The SDT contends that the new "Super ESP/ESZ" construct allows for cases where either routing cannot be used (such as layer 2 high speed database/ file replication) or where time sensitive data would be required to cross existing ESP boundaries (IEC-61850 GOOSE).