NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Virtualization Informal Posting Consideration of Comments

Project 2016-02 Modifications to CIP Standards

The standard drafting team (SDT) for Project 2016-02 Modifications to the CIP Standards, investigated the issues and unique risks associated with virtualization technologies. During the SDT's review, it was discovered that accommodating virtualization technologies in the CIP standards could affect many of the technical definitions, such as the foundational "Cyber Asset" used within CIP standards, and also the technical CIP standards (CIP-005, CIP-007, and CIP-010). Virtualization changes fundamental assumptions and some legacy standards requirements. There is no longer a need to prescribe the Electronic Security Perimeter (ESP) and Electronic Access Point (EAP) architecture with perimeter-based security or the exclusive use of routable protocol. The SDT found virtualization to be not only a driver of change, but also a pointer to a larger issue with the standards' adaptability to current and future technology innovation.

The SDT concluded that the more technical standards could benefit from removing inherent prescription of certain architectures and topologies, and moving requirements to an objective or results-oriented level that do not make assumptions about architecture. In other words, the SDT asserts that the standards should not prescribe how to secure today's newer architectures. Rather they should require that certain security objectives be met regardless of topology or architecture. In doing this, the standards will support virtualization and other future innovations that can increase reliability, resiliency, and security of our BES Cyber Systems.

The SDT posted the virtualization work that was completed to date for an informal posting November 2 to December 18, 2018. There were 76 sets of responses, including comments from approximately 199 different people from approximately 132 companies representing 10 of the Industry Segments.

The SDT thanks the industry for the time and attention given to these matters and the resulting comments. The SDT captured some of the overall themes from all the comments received to focus the SDT's efforts as we progress towards a formal posting.

Overall Themes

- Several commenters questioned the need for changes to requirements since virtualization is not prohibited and several entities have undergone successful audits on virtualized systems. An example of one of the fundamental issues would be when a Cyber Asset or an entire BES Cyber System and its associated systems (not only hosts, but storage, networks, EAPs, etc.) become logical constructs composed of software and data only. In response, the SDT will focus on communicating the case for change; why some changes are needed to allow different architectures and approaches that can significantly improve cyber security in virtualized environments but do not fit well with standards such as CIP-005. Virtualization technologies also present some unique risks that should be addressed.

- Commenters had suggestions on approaches they believe would help alleviate the amount of change to the current standards. The SDT will consider each approach as the team moves forward determining what changes can and should be made to the standards.
- Commenters pointed out some issues with the move away from the Cyber Asset level to a system level approach. They raised the concern this could cause an industry wide CIP-002 reassessment of all systems. They also pointed out that the systems concept has been used to group devices of like attributes (such as Operating Systems) for ease of reporting evidence on a per requirement basis. This type of grouping interferes with the concept of "Each BES Cyber System must be in a logical isolation zone." The SDT is considering how to incorporate changes based on these comments.
- Several commenters spoke to the security objective statements within the requirements. While there was support that objectives do provide clarity about the goal of a requirement, commenters suggested they are written too broadly, which introduces auditability concerns. The SDT will work towards drafting objective and measurable requirements.
- Almost all commenters responded to the removal of the term "programmable" within the definitions as we were looking at a full move to a systems approach. The concern was over the potential to bring in non-cyber components of systems such as electro-mechanical devices. The SDT will work on restoring the programmable terminology.
- Commenters suggested the Logical Isolation Zone (LIZ) concept needs further refinement and explanation. The SDT is considering refining this concept or identifying other options to clarify how security requirements will be applied within the standards.
- Commenters generally agreed with splitting out the 'monitoring only' portion of Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS) and treating that security risk at the information level. Some commenters suggested that the applicability of Electronic Access Monitoring Systems/Physical Access Monitoring Systems proposed in CIP-004 needs further review because it would continue to prevent the use of monitoring services. The SDT is continuing to consider options to allow monitoring information to be treated as BES Cyber Security Information to limit the scope of applicability.
- The proposed CIP Exceptional Circumstances (CEC) additions met with approval though several commenters suggested that all CEC phrasing should be at main requirement level. The SDT has considered this but must balance whether or not a CEC should be available for every requirement part. In those cases where the CEC does apply to every part it was moved to the main requirement.
- Many commenters suggested the Secure Configuration concept involved a fairly broad scope expansion from five discrete software items to numerous areas that would also include methods and processes. They believe that these would be difficult to inventory because they are not necessarily discrete items. Commenters suggested that several of the items in a Secure Configuration as defined are procedural, which conflicts with the change management requirement. Some pointed out that methods could differ per system, times thousands of systems. The SDT will continue to consider options to address the objective level requirement changes to limit the scope of change.