Background Information

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 a number of reasons for this, from the constraints of the current NERC CIP standards 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 Project 2016-02 Standard Drafting Team (SDT) was assigned the task to address the technological innovation in virtualization within the CIP standards.

This paper presents the SDT’s case for change to the NERC CIP standards. It discusses what is needed to allow for the innovative security techniques and new concepts brought about by virtualization. It outlines several technical areas where either prescriptive network topology in the standards or ambiguity around how to handle new security capabilities create issues. The paper then describes a high level way forward using new definitions for the virtualized environment. It also changes some requirements to technical security objectives, stating what security objective to achieve, but allowing the entity to choose the technology to accomplish it.

The SDT is interested in any comments you may have on the white paper.
Questions

1. Do you agree with the case for change based on the virtualization issues discussed in the white paper? Please provide comments.

   ☐ Yes  ☐ No

   Comments:
   At the executive level – 1) Expect the SDT to provide virtualization benefits; 2) Request the SDT also provide virtualization challenges – operational, cyber security and compliance.

   We are concerned that moving to “security objectives” will significantly impact auditors, starting with their training.

   Chapter 2 is an excellent start to the conversation of challenges in moving CIP to a virtualization

2. Do you agree with the proposed path forward as discussed in the white paper? Please provide comments.

   ☒ Yes  ☐ No

   Comments:
   Our concern is that although the example (figure 12) follows the model given it does not represent the complexity under which the industry has implemented CIPv5.

   We request the SDT post updates to CIP-007 and CIP-010 sooner. Those Requirements are the biggest hurdles. The industry and SDT will quickly see if the new Requirements will be acceptable.

   We support the proposed creation of new “shared infrastructure” and “virtual machine” cyber asset types and new “objective-based” type requirements specifically for those virtual cyber assets (as per Chapter 3) which would allow entities to adopt virtualization incrementally and at their discretion without changing existing CIP programs for entities that choose not to adopt virtualization.

   We request the SDT to describe how they plan to address mixed-use environments (hardware resources shared between CIP and non-CIP virtual machines).