NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

V5TAG Transfer Document Consideration of Issues

Project 2016-02 Modifications to CIP Standards Drafting Team

The September 2015 document entitled "CIP V5 Issues for Standard Drafting Team Consideration" ("V5TAG Transfer document") was included in the Standards Authorization Request (SAR) for the Project 2016-02 standard drafting team (SDT) to consider. This document contains the results of the SDT's review of each of these issues.

Cyber Asset Definition

The V5TAG asked the SDT to consider '...the definition of Cyber Asset and clarify the intent of "programmable" by considering factors such as whether or not a device is merely configurable, its executable code is not field upgradable, or if its functionality can only be changed via physical DIP switches, swapping internal chips, etc.'

The SDT posted the following proposed definition of "Cyber Asset" in March 2017 for industry comment:

> An electronic device (physical or virtual) whose operation is controlled by a stored program that can be changed or replaced by the end user, including the hardware, software, and data in the device. A virtual machine is itself a distinct asset from its host(s).

This proposed definition addressed both the 'programmable' issue and virtualization concerns. The industry comments on this proposal were weighted towards the negative. The concerns expressed were:

- It did not align with published NERC Lessons Learned documents from the V5TAG which have since been published as ERO endorsed Implementation Guidance.
- Any definition of 'programmable' would cause entities to initiate a compliance exercise to reevaluate every device for 'no measurable reliability benefit.'
- The clarifications proposed by the SDT such as "by the end user," "stored program," and "data in the device" raised even more questions and needed further clarification.

In the November 2017 informal posting, the SDT proposed moving the CIP standards away from a device level focus and towards a fuller embrace of the 'cyber system' concept as one way to handle any concerns with programmable devices. The comment responses, however, were overwhelmingly negative to the absence of the word 'programmable' because it removed a core feature of what a 'cyber' system is. It also raised major concerns regarding whether electro-mechanical devices and other 'non-programmable' or even 'non-cyber' devices would be included in the CIP scope.

With these comments in mind, the SDT will include the word 'programmable' in the 'Cyber Asset' definition and have it perform its previous foundational role. This also keeps the standards consistent with the term "programmable electronic devices" as used in Section 215 of the Federal Power Act. The SDT proposes to not define it further. These actions restore the core features of what a Cyber Asset is so non-cyber electro-mechanical devices are clearly out of scope. The SDT is convinced by industry comments that it should not attempt to further define the term programmable due to the concerns raised in the March 2017 posting. This term has stood in place for well over a decade, since Version 1 of the CIP standards. Any change now would cause a very large exercise that the SDT is convinced would provide no commensurate benefit to reliability.

BES Cyber Asset Definition

The V5TAG had the following 3 considerations for the BES Cyber Asset definition:

- Focusing on the definition so that it does not subsume all other cyber asset types (being defined purely in terms of impact means all other cyber assets within the CIP scope are also BES Cyber Assets and can create a "hall of mirrors" effect);
- Considering a lower bound to the term, "adverse impact;"
- Clarifying the double impact criteria (cyber asset affects a facility and that facility affects the reliable operation of the BES).

To help alleviate some of these concerns, the SDT posted a version of the standard and modified or proposed retirement of definitions to move the standard to a system level focus. The SDT proposed the retirement of "BES Cyber Asset" and the following modification to "BES Cyber System:"

> Any combination of hardware (including virtual hardware), software (including application virtualization), and data, regardless of redundancy, performing one or more reliability tasks that if rendered unavailable, degraded, or misused would result in adverse impact to one or more BES Facilities within 15 minutes.

The feedback from industry was similar to that received on "Cyber Asset." This is because Version 5 was a massive rewrite of the standards and the industry is still implementing all of V5 with the low impact BCS coming into scope in 2020. The industry has not had a chance to become accustomed to what it has now. It does not support another rewrite of CIP-002 scoping processes based on changes to these foundational terms and concepts. Addressing these foundational issues back from the V5TAG timeframe had an expiration date, after which every entity, the ERO, and the Regions had to accept the language in V5 and build large programs around a set of 'as-is' definitions and concepts. The SDT will address any necessary, additional changes to these definitions to handle virtualization concepts.

Network and Externally Accessible Devices (ERC, ESP, IRA)

The V5TAG transfer document asked the SDT to consider the concepts and requirements of Electronic Security Perimeters (ESP), External Routable Connectivity (ERC), and Interactive Remote Access (IRA) including:

- Clarifying the 4.2.3.2 exemption phrase "between discrete Electronic Security Perimeters." When there is not an ESP at the location, consider clarifying that the communication equipment considered out of scope is the same communication equipment that would be considered out of scope if it were between two ESPs.
- The word 'associated' in the ERC definition is unclear because it alludes to some form of relationship, but does not specifically define the relationship between the items. Striking 'associated' and defining the intended relationship would provide necessary clarity.
- Review of the applicability of ERC including the concept of the term "directly" used in the phrase "cannot be directly accessed through External Routable Connectivity" within the Applicability section. Also, consider the interplay between IRA and ERC.
- Clarify the IRA definition to address the placement of the phrase "using a routable protocol" in the definition and clarify with respect to Dial-up Connectivity.
- Address the Guidelines and Technical Basis sentence, "If dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies."

The SDT agrees that these can be clarified without a revamp of the standards and definitions, and without causing undue burden on the industry. The SDT will address the ESP issues and clarify the ERC/IRA issues where IP to serial conversion occurs.

Transmission Owner Control Centers Performing Transmission Operator Obligations

The V5TAG asked the SDT to consider the following areas:

- CIP-002-5.1, Attachment 1 Control Center criteria for additional clarity and for possible revisions of Transmission Owners' Control Centers (TOCC), particularly for small or lower-risk entities performing the functional obligations of a Transmission Operator (TOP). A potential revision could be a size for criteria 2.12, Control Centers performing the functional obligations of a TOP.
- Clarify the applicability of requirements to a TOCC that performs the functional obligations of a TOP, particularly if the TO has the ability to operate BES switches, breakers and relays. Review the corresponding Guidelines and Technical Basis of CIP-002-5.1, specifically, the "CIP-002-5" section paragraph starting with "Responsibility for the reliable operation of the BES is spread across all Entity Registrations." Include the table following that paragraph, the "High Impact Rating (H)" section, and the criterion bullets for Control Centers under the "Medium Impact Rating (M)" section.
- Review the definition of Control Center. If there are revisions planned, recognize possible impacts on operations and planning standards and/or glossary terms that include 'Control Center'.

- Review the language scope of "perform the functional obligations of" throughout the Attachment 1 criteria.

CIP-002-6 passed industry ballot and contained an updated 2.12 criterion for medium impact Control Centers. This modified criterion created a threshold for medium impact Control Centers and removed the "perform the functional obligations of" language.

In addition, the SDT posted a proposed modification to the definition of "Control Center" in April 2018 to address these areas during CIP-012-1 development. Based on comment responses, the SDT decided not to modify the definition.

Virtualization

The V5TAG transfer document stated:

> The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration.
>
> The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server, and storage virtualization technologies.

The SDT agrees and is considering revisions within the CIP standards to incorporate the concepts and risks unique to virtualized environments. In its approach, however, the SDT will not "make clear the permitted architecture." One of the current issues with CIP-005 and virtualization is that it defines and drives certain architectural decisions. That is not a role of these standards. The CIP standards should address the security risks without driving all entities to particular types of architecture in their systems. The SDT goal is to address virtualization in a way that is technology and architecture-agnostic and helps future-proof the standards.