NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

CIP Version 5 Revisions

Standard Drafting Team Update

Stakeholder Webinar
January 19, 2016

RELIABILITY | ACCOUNTABILITY

Administrative Items

- NERC Antitrust Guidelines
  - It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.
- Notice of Open Meeting
  - Participants are reminded that this webinar is public. The access number was widely distributed. Speakers on the call should keep in mind that the listening audience may include members of the press and representatives of various governmental authorities, in addition to the expected participation by industry stakeholders.

Webinar Topics

- Introduction
- Critical Infrastructure Protection (CIP) V5 Transition Advisory Group (TAG)
- Issues transferred to the CIP V5 Revisions Standard Drafting Team (SDT)
- Next Steps

CIP V5 Transition Advisory Group (V5TAG)

- On November 22, 2013, FERC approved CIP V5
- In 2014, NERC initiated a program to help industry transition from CIP V3 standards to CIP V5
- The goal of the transition program is to improve industry's understanding of the technical security requirements for CIP V5, as well as the expectations for compliance and enforcement
- CIP V5 Transition Program website: http://www.nerc.com/pa/CI/Pages/Transition-Program.aspx

CIP V5 Transition Advisory Group (V5TAG)

- V5TAG’s Role & Composition
  - Regional Entity Participants
  - Registered Entity Participation
  - NERC and FERC

- Consensus building through collaboration
  - Over 40 CIP V5 related topics addressed
    - Lessons Learned
    - Frequently Asked Questions
    - 4 topics transferred to the SDT

CIP V5 Transition Advisory Group (V5TAG)

- Recognition that standards development was needed for some issues that could not be resolved through compliance guidance
- Enhanced coordination with compliance and enforcement for topics being addressed via standards development
  - Facts and specific circumstances will dictate if violations will be identified to address areas of noncompliance for the related topics
  - Regional Entities will use Areas of Concerns and Recommendations to help identify risks associated with specific implementations
  - Feedback from industry will be used to help guide standard development activities

V5TAG and the CIP V5 Revisions SDT

- The CIP V5 Revisions SAR allows for the existing SDT to consider issues discovered during the transition to CIP V5
- V5TAG document provides starting information on which the SDT can build a scope of work for the future revision project. The SDT expects to use the stakeholder process to share scoping information in a transparent manner
- This webinar is to share information received to date
- A revision project will not begin before the April 1, 2016 CIP V5 deadline to allow for additional insights from the transition and to accommodate other factors

Cyber Asset and BES Cyber Asset Definitions

- The SDT should consider the definition of Cyber Asset and clarify the intent of "programmable"
- The SDT should consider clarifying and focusing the definition of "BES Cyber Asset" including:
  - Focusing the definition so that it does not subsume all other cyber asset types
  - Considering if there is a lower bound to the term 'adverse' in "adverse impact"
  - Clarify the double impact criteria (cyber asset affects a facility and that facility affects the reliable operation of the BES) such that "N-1 contingency" is not a valid methodology that can eliminate an entire site and all of its Cyber Assets from scope

Network and Externally Accessible Devices

- The SDT should consider the concepts and requirements concerning Electronic Security Perimeters (ESP), External Routable Connectivity (ERC), and Interactive Remote Access (IRA) including:
  - Clarify the 4.2.3.2 exemption phrase "between discrete Electronic Security Perimeters." When there is not an ESP at the location, consider clarity 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 in that it alludes to some form of relationship but does not define the relationship between the items. Striking 'associated' and defining the intended relationship would provide much needed clarity

Network and Externally Accessible Devices (cont.)

- The SDT should consider the concepts and requirements concerning Electronic Security Perimeters (ESP), External Routable Connectivity (ERC), and Interactive Remote Access (IRA) including:
  - 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. As well, 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 clarity 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.”

Transmission Owner (TO) Control Centers Performing Transmission Operator (TOP) Obligations

- CIP-002-5.1, Attachment 1 Control Center criteria for additional clarity and for possible revisions related to TOs' Control Centers performing the functional obligations of a TOP, in particular for small or lower-risk entities
- Clarify the applicability of requirements on a TO Control Center that perform the functional obligations of a TOP, particularly if the TO has the ability to operate switches, breakers and relays in the BES
- The definition of Control Center
- The language scope of "perform the functional obligations of" throughout the Attachment 1 criteria

Virtualization

- CIP V5 standards do not specifically address virtualization
- 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

Next Steps

- The CIP V5 Implementation continues
- The V5TAG also continues to discuss transition aspects
- Future CIP Revision project will not begin before April 1, 2016, but project planning is underway.
  - This timing is supported by the Standards Committee
- Among the many planning aspects are:
  - A nomination period will be enacted to fill SDT vacancies
  - Consideration of FERC Order to be issued on January 21, 2016
  - The recently approved Compliance Guidance Policy creates new opportunities to test implementation and compliance while developing requirement language

Information

- Senior Standards Developer, Steve Crutchfield
  - Email at stephen.crutchfield@nerc.net
  - Telephone: 609-651-9455

Questions