NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Meeting Notes
Project 2016-03 Cyber Security Supply Chain Risk Management Standards Drafting Team

March 9, 2017 | noon - 1:30 p.m. Eastern

Conference Call
1-415-655-0002 (US Toll)
1-416-915-8942 (Canada Toll)
Access Code: 8656-5311

Administrative

1. **Introductions**

   The meeting was brought to order by the Chair at noon eastern on March 9, 2017. The following SDT members and staff observers were on the conference call. Various stakeholder observers were also on the call:

First Name	Last Name	Company	Member/ Observer
Christina	Alston	Georgia Transmission	M
James	Chuber	Duke Energy	M
Norm	Dang	IESO	M
Shamai	Elstein	NERC	O
Chris	Evans	Southwest Power Pool	M
Brian	Gatus	SCE	M
David	Gayle	Dominion Resources	M
Scott	Mix	NERC	O
JoAnn	Murphy	PJM Interconnection	M
Mark	Olson	NERC	O
Skip	Peeples	Salt River Project	M

First Name	Last Name	Company	Member/ Observer
Corey	Sellers	Southern Company	M
Simon	Slobodnik	FERC	O
Jason	Witt	East Kentucky Power Cooperative	M

2. **Determination of Quorum**
   The rule for NERC Standard Drafting Team (SDT or team) states that a quorum requires two-thirds of the voting members of the SDT. Quorum was achieved as 10 of 11 members were present.
3. **NERC Antitrust Compliance Guidelines and Public Announcement**

   NERC Antitrust Compliance Guidelines and public announcement were reviewed by Mark Olson. There were no questions raised.
4. **Discuss themes from formal comments and consider potential solutions to address stakeholder concerns.** Participants discussed key issues that were observed in the comments from initial posting of CIP-013. The SDT agreed that the attached summary covers the stakeholder issues. SDT agreed that these issues reflected stakeholder concerns from the initial comment period for CIP-013. The SDT agreed that the March 14-16 in-person meeting would be approached by considering each issue, developing an SDT position, developing revisions to CIP-013-1 where appropriate, and determining other actions needed to address the stakeholder concern, where appropriate.
5. **Administrative information for the upcoming meeting was presented by Mark Olson.** The SDT agreed to also begin planning for an in-person meeting in early April.
6. **Future meeting(s)**
   a. March 14-16, 2017 | CPS Energy San Antonio
   b. TBD April 2017 | in-person meeting
7. The meeting adjourned at 1:15 p.m. eastern on March 9, 2017

Summary of Stakeholder Issues

The list below contains topics/issues raised by stakeholders during the initial commenting for draft CIP-013-1. The SDT will consider the issues and develop: (i) SDT position; (ii) revisions to draft CIP-013, where appropriate, (iii) additional actions to address stakeholder issues, where appropriate.

Overview

1. Does Order 829 limit the requirements to pre-operation (i.e., “supply chain” only) activities?
    a. Need to explicitly define "Supply Chain" (pre-operation); limit requirements based on this definition

R1

1. Scope of "BES Cyber Systems and, if applicable, associated EACMS, PACS, and PCAs" is beyond scope of Order
    a. Focus on “industrial control system” vendors
    b. Split requirement based on High, Medium, Low categories – apply R1 to Highs/Mediums only; move Lows to CIP-003 or delete Lows altogether
2. Need to explicitly identify the risks to evaluate or define the security objective(s)
3. Need specific language addressing applicability to future contracts only OR language stating clearly “no renegotiation or abrogation of existing contracts”
4. Address specific evidence of compliance with R1 (specific measures)
    a. Include "obtaining specific controls in the negotiated contract may not be feasible and is not considered failure [to comply]..." in R1
    b. Introduce “where technically/contractually feasible” language or a concept similar to Technical Feasibility Exceptions

R2

1. Need to be clear on what NERC/DHS “guidance” should be considered – list is too vague and open-ended
    a. Consider including Rationale examples in requirement
2. Clarify that plan is updated every 15 months, not after each new potential risk/vulnerability is identified
3. Consider removing subparts 2.1/2.2 – collapse into R2 language
    a. Part 2.1 is not needed-consider rewording into a single requirement
    b. Consider making R2 part of R1
4. First approval of Supply Chain Plan(s) is not required until review/revisions cycle

5. Approval by delegates is not aligned with CIP-003
6. Clarify ***as necessary*** where used in the requirement

R3

1. More appropriate to address directives in other standards
2. Potential negative impact on reliability - may negatively impact ability to patch systems in the required timeframe for CIP-007 R2.3
3. TFE or rewording needed to provide flexibility for asset or vendor capability
4. Overlap with approved CIP standards - remove parts that are duplicative
5. Scope should be revised:
    a. limited to assets "with externally routed connectivity and dial-up"
    b. include EACMS, PACS, PCA, etc
6. Use a table to define scope
7. Duplicative of R1

R4

1. More appropriate to address directives in other standards
2. TFE or rewording needed to provide flexibility for asset or vendor capability
3. Overlap with approved CIP standards - remove parts that are duplicative
4. Clarify (or define) system-to-system; be consistent in standard/rationale/guidance
5. Clarify “unauthorized activity"; consider change to "unauthorized access"
6. Consider changing 'monitoring' to 'controlling'
7. Respond v. disable

R5

1. R5 should be removed
    a. Focus should only be on “supply chain” – stop short of operational requirements
    b. Order focuses on risk-based approach – by definition Lows are not critical and Low operational requirements are unneeded
2. No clear way to comply or provide evidence without a list – requiring an inventory of Low assets is in conflict with existing CIP standards
3. Any Low impact asset requirements should be moved to CIP-003
4. Overlap/confusion between R1 and R5 – clarification is needed
5. R5 should apply to Entities with "low impact BES Cyber Systems" only
6. Having a “policy” for Lows is not enough – need to implement the policy

Implementation Plan

1. Longer implementation time is needed
2. Implement in phases