NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2016-02 CIP Modifications

November 2016 Standard Drafting Team (SDT) Meeting Summary

December 2, 2016

RELIABILITY | ACCOUNTABILITY




SDT Meeting Activities

- Covered administrative details and confirmed quorum.
- Team conducted a webinar on the following:
  - LERC Definition and CIP-003-7 (posted for formal comment/ballot)
  - Transient Cyber Assets (TCA) at Lows (posted for informal comment)
- Team discussed in detail the following issue areas:
  - CIP Exceptional Circumstances (CEC)
  - Virtualization
  - Definitions and Concepts
  - Transmission Owner (TO) Control Centers performing the function of a Transmission Operator (TOP)
  - Communication Networks between Control Centers Informal Posting
  - Transient Cyber Assets at Lows (Definition of Removable Media)

Key Messages

- The LERC revisions are posted for stakeholder comment and ballot until December 5, 2016.
- TCA revisions posted for informal comment until Nov 18, 2016.
- SDT approved a package of materials, including edits from QR, on Communication Networks between Control Centers for informal posting. Target posting date for later in November.
- SDT continues to move toward informal postings for the CIP Exceptional Circumstances and Transmission Owner Control Center issue areas.
- Substantial work continues investigating the definitions & concepts and virtualization issue areas.

CIP Exceptional Circumstances

- The SDT reviewed two options for CIP Exceptional Circumstances (CEC), a requirement-based approach (option 1) and a programmatic approach (option 2):
  - Option 1:
    - Retains the existing CIP Exceptional Circumstance language in the currently approved Requirements and includes the same language to select, additional Requirements.
    - With this approach, the Responsible Entity is not required to perform the obligation of the requirement language when experiencing a CIP Exceptional Circumstance, but must follow the elements outlined in their cyber security policy pursuant to CIP-003-6 R1.

CIP Exceptional Circumstances

- Option 2:
  - Creates Requirement 5 within CIP-003 to allow for a programmatic approach to identifying, declaring, and documenting CIP Exceptional Circumstances.
  - This programmatic approach is intended to support consistent evaluation of the impact a CIP Exceptional Circumstance may have on a Responsible Entity.
  - The facts and circumstances of the CIP Exceptional Circumstance provide key information to assessing the risk of any noncompliance, which would include consideration as a compliance exception through the ERO's risk-based Compliance Monitoring and Enforcement Program.
  - Placement of this requirement in CIP-003 also allows for application to assets identified in CIP-002 containing low impact BES Cyber Systems.

- Based on the discussion, the SDT plans to recommend the use of Option 1.
- An informal comment is planned to gain industry feedback.

Virtualization

- The subteam reviewed the risk map which identifies:
  - Risks associated with virtual systems
  - Alignment to current CIP Standard Requirements
- The subteam led discussion on mixed use Cyber Assets
- Action Items
  - Subteam to complete risk map including description and rationale
  - Subteam to identify tasks requiring feedback from broader participation

Definitions and Concepts

- The SDT reviewed the Cyber Asset, BES Cyber Asset, and BES Cyber System definitions.
  - Differences were highlighted between data center environments and field environments, such as plants and substations.
- The SDT discussed more fully leveraging the systems approach towards securing Cyber Assets with limited capabilities as intended under the CIP V5 structure.
- The SDT reviewed the definitions of Electronic Security Perimeter (ESP), External Routable Connectivity (ERC), Interactive Remote Access (IRA), and Electronic Access Control and Monitoring Systems (EACMS).
- The SDT also reviewed options for modifying the exclusion for communication networks between discrete ESPs to account for locations where an ESP is not required.

Transmission Owners performing the function of a Transmission Operator

- The subteam working on the Transmission Owners performing the function of a Transmission Operator issue area circulated an early draft whitepaper outlining the research the team has performed and solutions under consideration.
- Once complete, the SDT plans to post the whitepaper for an informal stakeholder comment period.
- The SDT reviewed and edited the questions posed for the informal comment period.

Communication Networks between Control Centers

- The SDT reviewed the QR feedback on the draft and approved the documents to move forward with informal posting.
- The proposal package includes:
  - Draft of Standard CIP-012
  - Comment form
- Proposal package will be posted following the LERC ballot and will close on January 13th.

Transient Cyber Assets at Lows – Definition of Removable Media

- During the industry webinar, the SDT received a question from a stakeholder asking why modifications to the definition of Removable Media were not made consistent with those of the Transient Cyber Asset definition (as proposed in the informal posting).
- The SDT anticipated that this would be a common question raised during the informal comment period on the draft TCA requirements.
- In response, the SDT drafted and approved a modification to the Removable Media definition to be included when the standard is submitted for formal comment and ballot.

Transient Cyber Assets at Lows – Definition of Removable Media

- The modified definition of Removable Media is as follows:

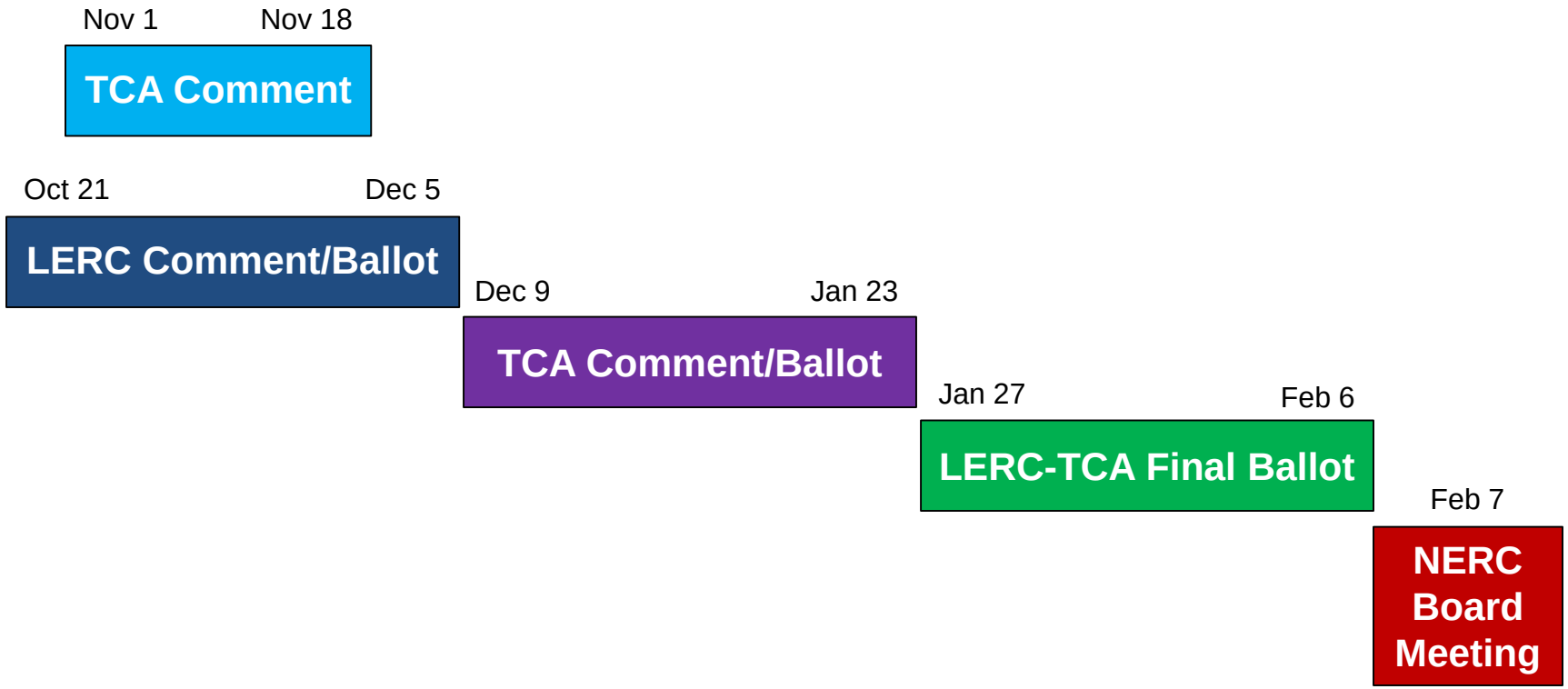
  Storage media that:

  1. are not Cyber Assets,
  2. are capable of transferring executable code,
  3. can be used to store, copy, move, or access data, and
  4. are directly connected for 30 consecutive calendar days or less to a:
     - BES Cyber Asset, ~~a~~
     - network within an Electronic Security Perimeter (ESP)~~,~~ containing high or medium impact BES Cyber Systems, or ~~a~~
     - Protected Cyber Asset associated with high or medium impact BES Cyber Systems.

  Examples of Removable Media include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

Potential Posting Schedule

- If the LERC and TCA revisions pass stakeholder ballot and final ballot, all revisions could be presented to the Board in February for adoption.



Next Steps

- Review TCA comments and determine status of formal posting
- Prepare for CIP-003-7 (LERC) comments/ballot and final ballot
- Prepare to post CIP-012 - Communication Networks between Control Centers for Informal Comment Posting
- Continue development of Transmission Owner (TO) Control Centers performing the function of a Transmission Operator (TOP) Whitepaper for Informal Comment Posting
- Prepare CIP Exceptional Circumstances (CEC) proposal for Informal Comment Posting
- Continue research and analysis on Virtualization
- Continue research and analysis on Definitions and Concepts

Conference Call Schedule

Conference Call Dial-In

- 866-740-1260
- access code 5301963

Reserved Call Times

- Tuesdays - Noon – 2 p.m. (ET)
  - security code 0001
- Thursdays - Noon – 2 p.m. (ET)
  - security code 0003
- Fridays - 11 a.m. – 1 p.m. (ET)
  - security code 0005

- Discussion topics will vary based on the issue area work progress.
- Calls may be cancelled to allow the sub-teams to process input and develop proposals.
- Notifications of the call schedule are sent weekly to the Project Plus List.

SDT Meeting Schedule

2016 Meeting Schedule:

- December 6-8, 2016 – Orlando, FL - Orlando Utilities Commission,

2017 Planned Dates :

- January 24-26 – New Orleans, LA - Entergy
- February 21-23 – St. Petersburg, FL – Duke Energy
- March 21-23 – Houston, TX - Occidental Energy Ventures
- April 18-20 – Tampa, FRCC
- May 23-25 – Columbus, OH - American Electric Power
- June 20-22
- July 18-20
- August 22-24
- September 19-21
- October 10-12
- November 14-16

Resources

- This slide deck and other information relative to the CIP Modifications SDT may be found on the Project 2016-02 Project Page under Related Files:

  Project 2016-02 Modifications to CIP Standards

Questions and Answers