NERC CIP Standards Update – Item 3

Project 2016-02 – CIP Modifications
Project 2019-02 – BCSI Access Management
Project 2019-03 – Cyber Security Supply Chain Risks

Nov 26, 2020

ieso
Connecting Today.
Powering Tomorrow.

CIP Updates

- 2016-02 SDT CIP Modifications - Virtualization Update
- 2019-02 SDT BCSI Access Management
- 2019-03 SDT Cyber Security Supply Chain Risks

Coordination Between CIP SDTs

In order to prevent confusion due to the large number of CIP Standards being changed:

- Project 2019-03 SDT (Supply Chain) has completed their work
- Project 2019-02 SDT (BCSI in Cloud) is working on making changes to CIP-004-6 and CIP-011-2 (leaving EACMS)
- Project 2016-02 SDT will work with 2019-02 SDT for conforming changes to CIP-004 and CIP-011

2016-02 CIP Mods - Virtualization Update

- Half day long workshop was held Sept 30
- Introduced the proposed language virtualization requirements language for CIP-005, CIP-007 and CIP-010
- Feedback via “slido” interactive poll was generally positive
- The SDT will address the themes of questions presented
- SDT is proceeding to modify the remaining CIP-002 to CIP-013 for conforming language
- 2016-02 SDT will coordinate with 2019-02 SDT in modifications for CIP-004 and CIP-011
- 2016-02 SDT will post entire suite of CIP-002 – CIP-013 with virtualizations changes late Jan – early Feb 2021

2019-02 SDT BCSI Access Management

- The SDT has posted Draft 2 of CIP-004-7 and CIP-011-3 on Sept 21, 2020
- Draft 2 did not pass
- SDT is reviewing the comments and is incorporating these into Draft 3
- Main issues were around proposals :
  - CIP-004 “provisioned access list” vs “actual access list”
  - CIP-011 “methods” vs. “technical controls” (R1.2 vs R1.4)
- It is anticipated that Draft 3 will be posted for ballot in early 2021

2019-03 SDT Cyber Security Supply Chain Risks (Future)

- Final ballot of Standards CIP-013-2, CIP-005-7 and CIP-010-4 closed on Oct 16, 2020
- Passed – 76% with 83% quorum
- Regulatory filing due Dec 26, 2020

Standards – Effective Dates

- October 1, 2020 (Original July 1, 2020)
  - Original Supply Chain Standards CIP-005-6, CIP-010-3, CIP-013-1
- Future - January 1, 2021
  - Cyber Incident Reporting Standards CIP-008-6 – Attempted Cyber Security Incidents
- Future - April 1, 2022 (tentative)
  - Communications between Control Centers CIP-012-1 – Encryption of data links