RELIABILITY FIRST

Low Impact Focus Group

April 20, 2018

Opening Comments

- **This meeting is being recorded**
- **All lines will be muted.**
- **In order to comment, you may:**
  - Use the WebEx “Raise Hand” feature.
  - Send a message to the presenter via WebEx chat.
- **When commenting, be mindful that this is an open call. RF cannot fully pre-screen the attendees.**

Announcements

- **NERC's Antitrust Guidelines are available at:**
  - http://www.nerc.com/pa/Stand/Resources/Documents/NERC_Antitrust_Compliances_Guidelines.pdf
- **This is a public call. RF cannot fully pre-screen the attendees.**

Mailing List

- ciplifg@lists.rfirst.org
- This list is intended as a discussion forum.
- List changes, such as additions or removals, should be sent to: lew.folkerth@rfirst.org

Standards Update – FERC Order 843

- **On April 19, 2018, FERC issued Order 843**
  - Order is effective 60 days after publication in the Federal Register – on or about June 24, 2018
  - Approved CIP-003-7
  - Approved Implementation Plan
  - Did not order revisions to Section 3
  - Ordered a study of the effectiveness of Section 3 to be completed by 12/25/2019
  - Ordered modification of Section 5 to address malware found on vendor systems

Standards Update – FERC Order 843

➢ Summary of CIP-003-7

- Modified Attachment 1 Sections 2 and 3 to remove references to LERC and LEAP
- Removed the Glossary terms LERC and LEAP
- Added Attachment 1 Section 5 covering Transient Cyber Assets for low impact BES Cyber Systems
- Modified R1 Part 1.2.3, policy topic for electronic access controls
- Added R1 Part 1.2.5, policy topic for Transient Cyber Assets
- Added R1 Part 1.2.6, policy topic for CIP Exceptional Circumstances

Standards Update – FERC Order 843

➢ Implementation Plan

- Effective date of CIP-003-7 is first calendar quarter that is 18 months after the effective date of Order 843
  - January 1, 2020
- Effective dates for CIP-003-6 remain except for:
  - Attachment 1 Sections 2 and 3
    - Effective date is same as CIP-003-7
- Categorization changes remain subject to the Implementation Plan provisions for CIP-003-5 and CIP-003-6

Standards Update – FERC Order 843

➢ Implementation Considerations

- Electronic Access Controls
  - "[M]ust document the necessity of its inbound and outbound electronic access permissions and provide justification of the need for such access." [P22]
  - "[P]rovides a clear security objective that establishes compliance expectations." [P27]
  - "[i]f a Responsible Entity fails to articulate a reasonable business or operational need for the electronic access permission, the ERO Enterprise would find that the Responsible Entity did not comply with Section 3.1." [P22]
  - "We expect responsible entities to be able to provide a technically sound explanation as to how their electronic access controls meet the security objective." [P28]

Standards Update – FERC Order 843

➢ Implementation Considerations

- Transient Cyber Assets
  - "[T]o achieve the objective of mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets or Removable Media." [CIP-003-7 Att 1 Section 5]

Low Impact Summary

Summary of Low Impact CIP Requirements

Standard/Requirement	Effective Date	Description
CIP-002-5.1 R1 Part 1.3	7/1/2016	Low impact BES Cyber System identification (asset level)
CIP-003-6 R1 Part 1.2	4/1/2017	Policy for low impact BES Cyber Systems
CIP-003-7 R1 Part 1.2	1/1/2020	Policy for electronic access controls, TCA, CIP Exceptional Circumstances
CIP-003-6 R2	4/1/2017	Calls Attachment 1 into scope for low impact BES Cyber Systems
CIP-003-6 Att 1 Section 1	4/1/2017	Security awareness
CIP-003-7 Att 1 Section 2	1/1/2020	Physical access controls
CIP-003-7 Att 1 Section 3	1/1/2020	Electronic access controls
CIP-003-6 Att 1 Section 4	4/1/2017	Cyber Security Incident response plan
CIP-003-7 Att 1 Section 5	1/1/2020	Transient Cyber Assets
CIP-003-6 R3	7/1/2016	Designation of CIP Senior Manager
CIP-003-6 R4	7/1/2016	CIP Senior Manager delegations
CIP-004 to CIP-011	N/A	Not applicable to low impact BES Cyber Systems
CIP-012-1	TBD	Control Center communications - under development - ballot open
CIP-013-1	N/A	Not applicable to low impact BES Cyber Systems
CIP-014-2	10/2/2015	Physical security

Note: Some dates were corrected from the recorded presentation.

Additional Topics

➢ VOIP

- "Our control center and wind farms utilize VoIP systems to communicate with each other and to other regulatory entities. From reading CIP guidance, it appears that the VoIP systems could be classified as a BES Cyber asset, but yet be outside the scope of CIP-002 due to the location of the VoIP router. Our VoIP router is not currently behind the firewall, which is what we define as the Electronic Access Point. Do you know how other low impact entities are addressing VoIP systems? Are they classifying them as BES Cyber Systems? If so, do you know why? Also, how are they implementing the LEAP associated with VoIP?"

Future Meetings

- **Next conference call (WebEx):**
  - As needed

Questions & Answers

Forward Together ReliabilityFirst