NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Project 2016-02 – Modifications to CIP Standards

Technical Conference
April 19, 2016
Atlanta, GA

RELIABILITY | ACCOUNTABILITY




# Agenda

- Welcome – Steven Noess
- NERC Antitrust Compliance Guidelines and Public Announcement* - Al McMeekin
- Logistics and safety awareness – Ryan Stewart
- Industry Training on CIP standards approved in Order 822 - Scott Mix
- FERC Order 822 Directives – Stephen Crutchfield
- CIP V5TAG Issues – Tobias Whitney
- Wrap-up and next steps – Al McMeekin

# 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.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# CIP Version 6-2 Reliability Standards

## Overview of Recently Approved Changes

Scott R. Mix, CISSP, Sr. CIP Technical Manager, NERC

Technical Conference
April 19, 2016
Atlanta, GA

RELIABILITY | ACCOUNTABILITY




# Agenda

- Responses to Four FERC Directives
  - Identify, Assess and Correct
  - Transient Devices
  - Communication Networks
  - Low Impact Requirements
- Effective Dates

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Responses to FERC Directives Identify, Assess, and Correct

# Identify, Assess, and Correct

- FERC preferred to not have “compliance language” included within technical requirement
- SDT responded by deleting language from 17 requirements
- RAI (Risk-based Compliance Monitoring and Enforcement) concepts replaced need for IAC language
  - Identification > exception tracking and self reports
  - Assessment > risk assessment guidance
  - Correct > incentives to not recur exceptions or non-compliances
- No additional requirements introduced

# Responses to FERC Directives Transient Devices

# Transient Devices

- Described in Final Rule as devices connected for less than 30-days (USB, laptop, etc.)
- FERC directed modifications to address the following concerns:
  - Device authorization
  - Software authorization
  - Security patch management
  - Malware prevention
  - Unauthorized physical access
  - Procedures for connecting to different impact level systems

# Transient Devices

- SDT developed two additional definitions:
  - Removable Media
  - Transient Cyber Assets
- Modified CIP-004 Part 2.1 to address training on risks associated with Transient Cyber Assets and Removable Media

# Transient Devices

- **Transient Cyber Asset**: A Cyber Asset that (i) is capable of transmitting or transferring executable code, (ii) is not included in a BES Cyber System, (iii) is not a Protected Cyber Asset (PCA), and (iv) is directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless, including near field or Bluetooth communication) for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a PCA.

Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

# Transient Devices

- **Removable Media**: Storage media that (i) are not Cyber Assets, (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a Protected Cyber Asset.

Examples 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.

# Transient Devices

- CIP-004-6 Requirement R2
  - Part 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with Removable Media

# Transient Devices

- Added CIP-010 Requirement R4 dealing with issue
  - Detailed requirements in attachment and measures in a separate attachment
  - Separated into three areas:
    - Transient Cyber Assets managed by Responsible Entity
    - Transient Cyber Assets managed by other parties
    - Removable Media

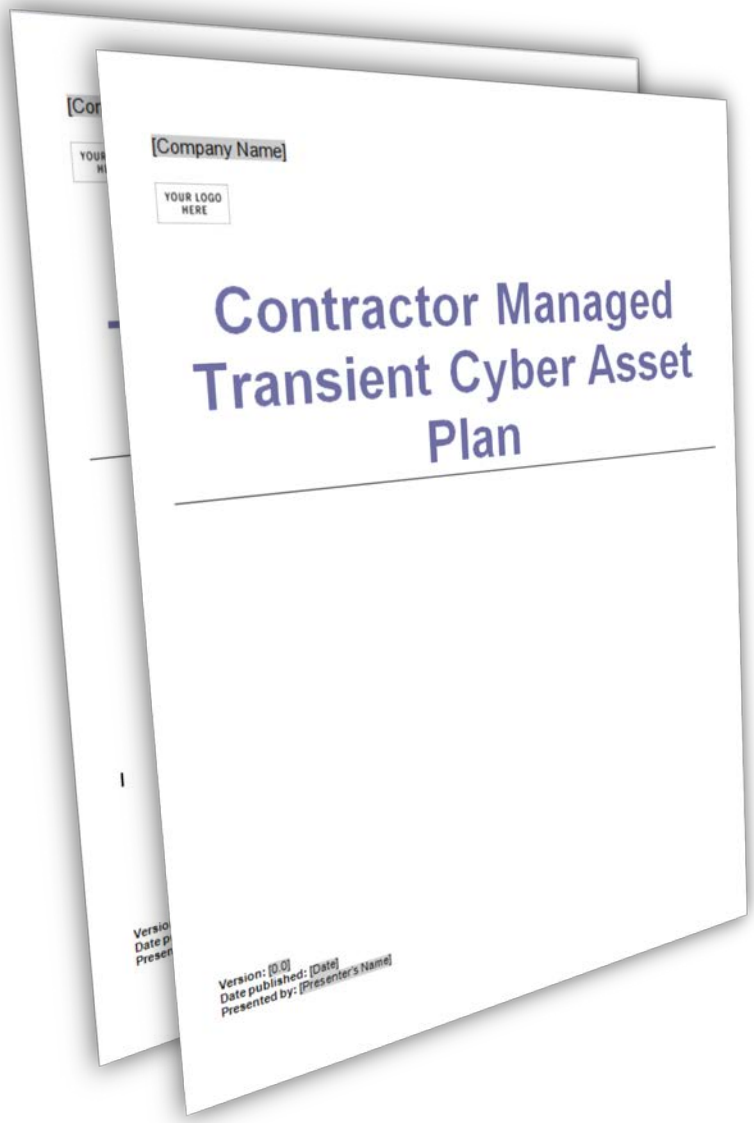
# Responsible Entity Managed Transient Cyber Assets


- Transient Cyber Asset Management
  - Ongoing
  - On-demand
- Transient Cyber Asset Authorization
  - Users
  - Locations
  - Uses
- Security Vulnerability Mitigation
  - Patching
  - Hardening
  - Read-only media
- Introduction of Malicious Code Mitigation
- Unauthorized Use Mitigation
  - Physical restriction
  - Encryption
  - Multi-factor authentication

# Approach #1 – "On Demand"

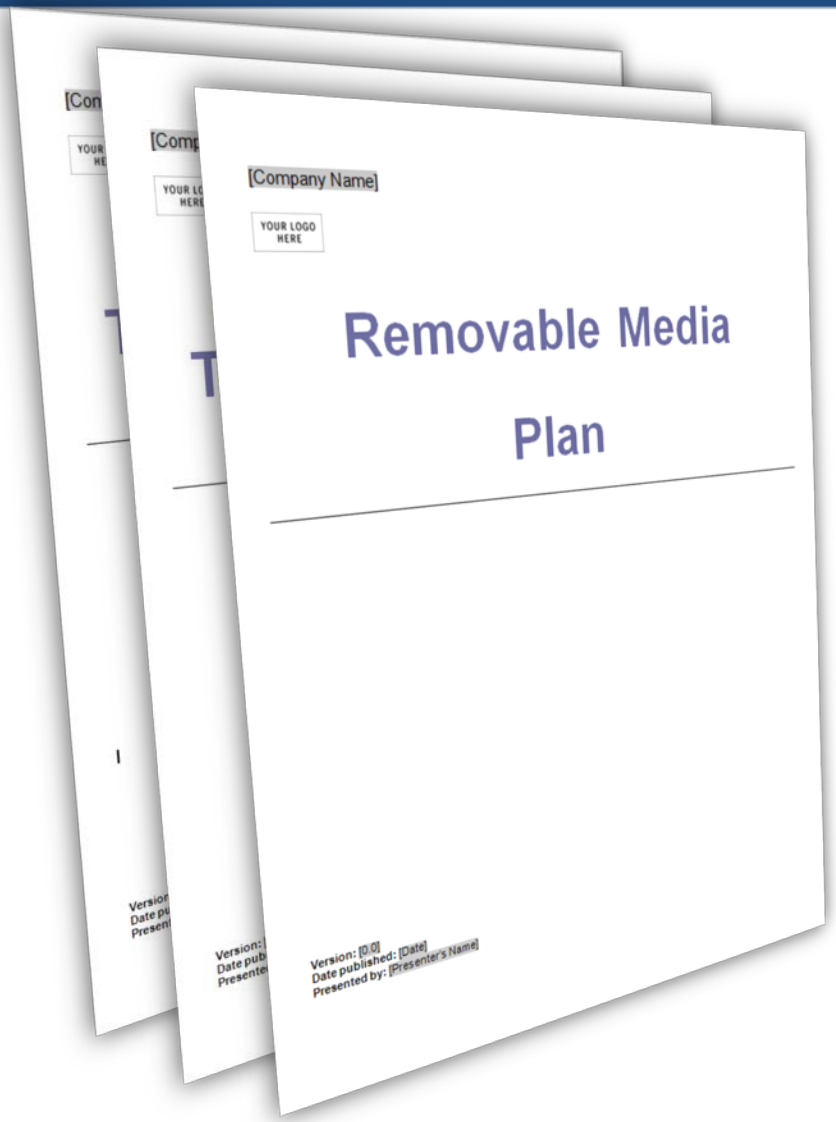
# Approach #2 – "Ongoing" Management

# Contractor Managed Transient Cyber Assets




- Security Vulnerability Mitigation
  - Review of contractor's implementation
- Introduction of Malicious Code Mitigation
  - Review of contractor's implementation
- Review of need for additional mitigation actions

# Removable Media




- Removable Media Authorization
  - Users
  - Locations
- Malicious Code Mitigation
  - Detect
  - Mitigate

# Responses to FERC Directives Communication Networks

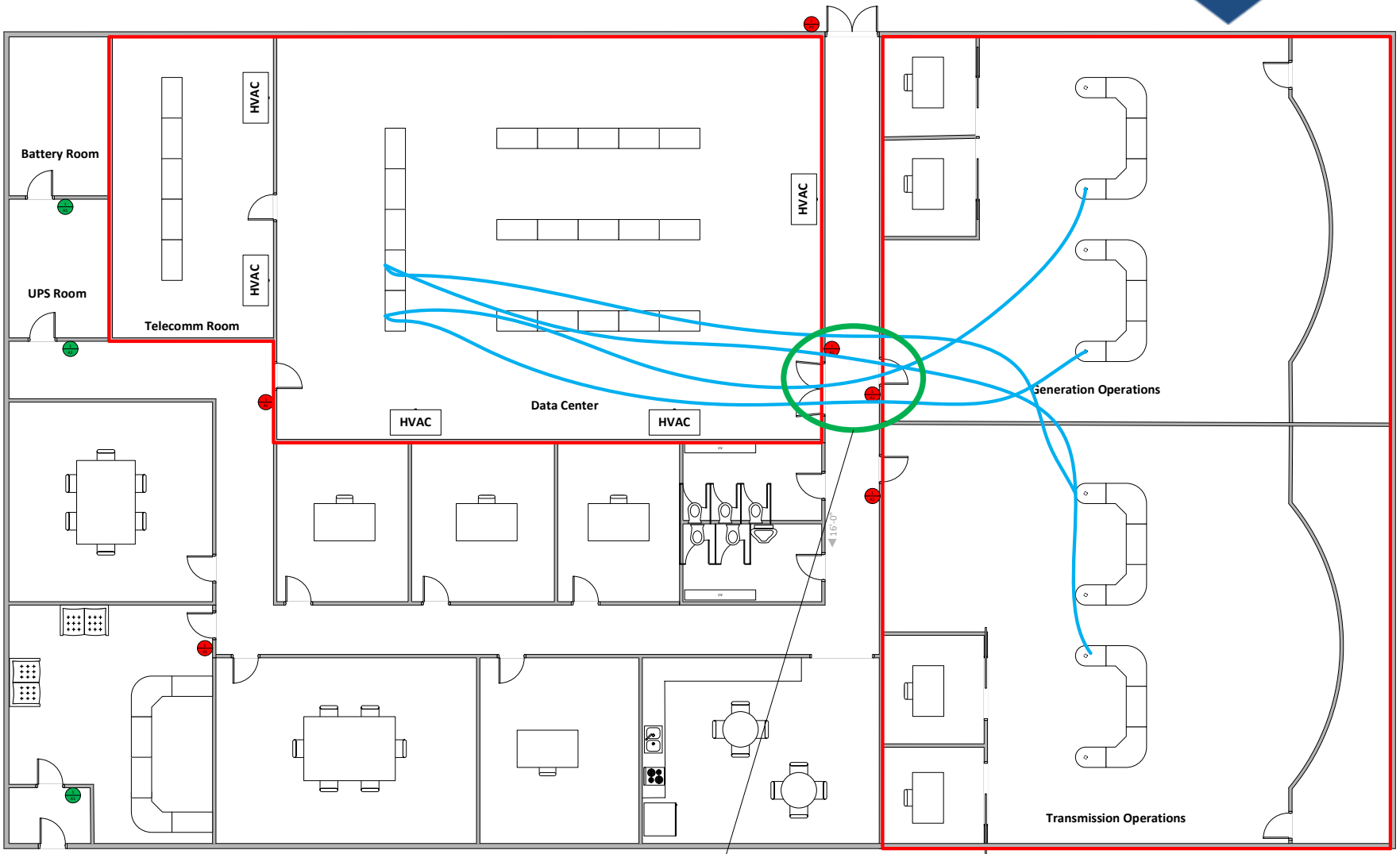
# Communication Networks

- FERC Directed creation of definition of “communication networks” and requirements to address issues:
  - Locked wiring closets
  - Disconnected or locked spare jacks
  - Protection of cabling by conduit or cable trays

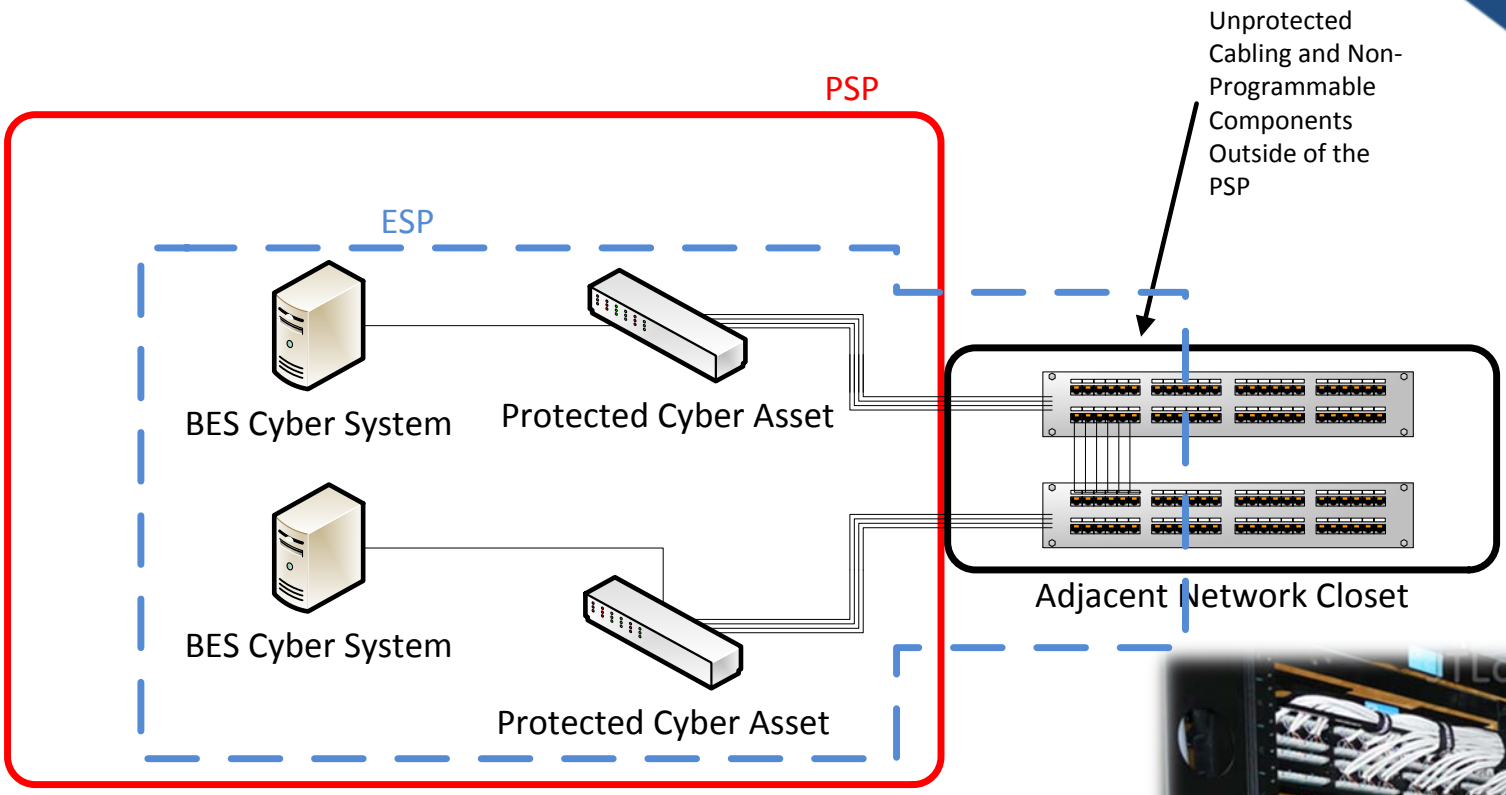
# Communication Networks

- SDT responded by adding CIP-006 Part 1.10 to address protections of "non programmable" components of communication networks that are inside an ESP, but outside of a PSP by
  - Encryption of data that transits such cabling and components; or
  - Monitoring the status of the communication link composed of such cabling and components and issuing an alarm or alert in response to detected communication failures to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection; or
  - An equally effective logical protection
- In this context, "non programmable" means components that are not Cyber Assets
  - Ports (e.g., on patch panels, wall jacks, port savers)
  - Cabling, couplers
  - Cable taps, media converters
  - Unmanaged switches (??), unmanaged hubs

# Communication Networks



# Communication Networks

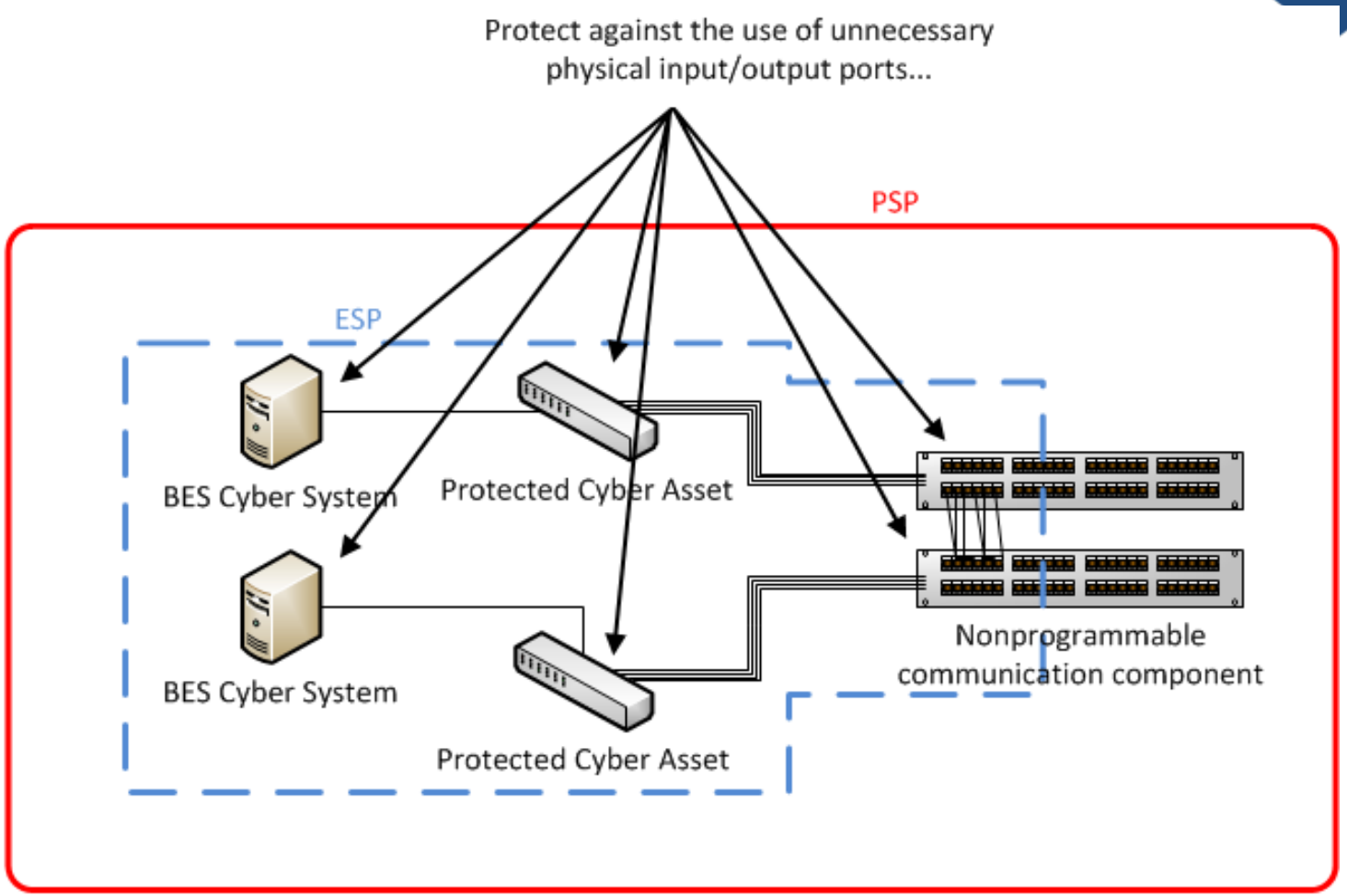



High Impact & Medium Impact Control Centers

# Communication Networks

- SDT also modified CIP-007 Part 1.2 to address unused physical ports on nonprogrammable communication components and devices at high and medium impact Control Centers
- Formal definition determined by SDT to be unnecessary at this time

# Communication Networks




High Impact & Medium Impact Control Centers

# Responses to FERC Directives Low Impact Requirements

# Low Impact Requirements

- FERC concerned with lack of objective criteria for evaluating Low Impact protections
  - "Introduces unacceptable level of ambiguity and potential inconsistency into the compliance process"
  - Open to alternative approaches
  - "… the criteria NERC proposes for evaluating a responsible entities' protections for Low impact facilities should be clear, objective and commensurate with their impact on the system, and technically justified."
- No detailed inventory required … list of locations /facilities OK

# Low Impact Requirements

- SDT maintained all low impact requirements in CIP-003
  - "Low-only entities" only need to comply with CIP-002 and CIP-003
- Added CIP-003 Part 1.2 dealing with security policy for low impact BES Cyber Systems
  - Policy Statements for the four "areas"
- Added attachments dealing with the technical requirement and measures
  - Kept four original "areas"

# Low Impact Requirements

- Security Awareness
  - "… reinforce, at least every 15 calendar months, cyber security practices…"
- Incident Response
  - Modeled from medium impact
  - 6 elements (of 9: collapsed process requirements and update requirements together; no documentation of deviations or specific record retention – but still need to demonstrate compliance)
- Physical Security
  - "…control physical access based on need…"
  - Includes locations containing LEAP devices
- Note – Common programs and procedures for high/medium and low *are* allowed, and should be noted when explaining to auditors

# Low Impact Requirements

**Section 4.** Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

**4.1** Identification, classification, and response to Cyber Security Incidents;

**4.2** Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law;

**4.3** Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

**4.4** Incident handling for Cyber Security Incidents;

**4.5** Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

**4.6** Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

# Low Impact Requirements

- Electronic Security
  - Two new definitions – LERC and LEAP
  - Similar to but different from ERC and EAP concepts at medium & high
  - Flexibility in the location of the "Cyber Asset containing the LEAP" that does not exist at high and medium
- "…permit only necessary inbound and outbound bi-directional routable protocol access…"
- "…authentication for all Dial-up Connectivity…"
- Seven "reference model" drawings showing LERC & LEAP in Guidelines and Technical Basis section
- Common programs make more sense for electronic security

# Low Impact Requirements

- ***ERC - External Routable Connectivity*** - The ability to access a BES Cyber System from a Cyber Asset that is *outside of its associated Electronic Security Perimeter* via a bi-directional routable protocol connection.

- ***LERC – Low Impact External Routable Connectivity*** - *Direct* user-initiated interactive access or a *direct* device-to-device connection to a low impact BES Cyber System(s) from a Cyber Asset *outside the asset* containing those low impact BES Cyber System(s) via a bi-directional routable protocol connection. Point-to-point communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions between Transmission station or substation assets containing low impact BES Cyber Systems are excluded from this definition (examples of this communication include, but are not limited to, IEC 61850 GOOSE or vendor proprietary protocols).

# Low Impact Requirements

- ***EAP - Electronic Access Point*** - A Cyber Asset interface on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.

- ***LEAP – Low Impact BES Cyber System Electronic Access Point*** - A Cyber Asset interface that controls Low Impact External Routable Connectivity. The Cyber Asset containing the LEAP may reside at a location external to the asset or assets containing low impact BES Cyber Systems.

# Effective Dates

# Effective Dates

- Phased implementation plan filed with the commission:
  - IAC – no proposed change (i.e., 4/1/16 or 3 months after approval)
  - Communication Networks – 9 months after the effective date of the standard
  - Transient Devices – 9 months after the effective date of the standard
  - Low Impact
    - Latter of 4/1/17 or 9 months after the effective date of the standard for policy, plan, security awareness, and response
    - Latter of 9/1/18 or 9 months after the effective date of the standard for physical and electronic security
- FERC Order No. 822 was effective on March 31, 2016, which is the basis for calculating all dates

# Effective Dates

- Trades Associations petition to align all high impact and medium impact dates – granted on February 25, 2016
  - All “existing” high and medium impact dates moved to July 1, 2016 (includes Identify, Assess, and Correct” language)
  - As a result, the basis for calculating dates moved to July 1, 2016
  - Transient device and Communication Networks – nine months after July 1, 2016, or April 1, 2017
  - Low impact dates unchanged by request

# Questions and Answers

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Project 2016-02 – Modifications to CIP Standards

Order 822 Directives

RELIABILITY | ACCOUNTABILITY




# FERC Order 822

- *32. Accordingly, we direct that NERC, pursuant to section 215(d)(5) of the FPA, develop modifications to the CIP Reliability Standards to provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to bulk electric system reliability. While NERC has flexibility in the manner in which it addresses the Commission's concerns, the proposed modifications should be designed to effectively address the risks posed by transient devices to Low Impact BES Cyber Systems in a manner that is consistent with the risk-based approach reflected in the CIP version 5 Standards.*

# FERC Order 822 Paragraph 32

- *Is the directive clear and well understood?*
- *Do you have any suggestions on ways to address the directive?*

# FERC Order 822

- *53. Therefore, we adopt the NOPR proposal and direct that NERC, pursuant to section 215(d)(5) of the FPA, develop modifications to the CIP Reliability Standards to require responsible entities to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact).*

# FERC Order 822

- 56. NERC's response to the directives in this Final Rule should identify the scope of sensitive bulk electric system data that must be protected and specify how the confidentiality, integrity, and availability of each type of bulk electric system data should be protected while it is being transmitted or at rest.

# FERC Order 822 Paragraphs 53 / 56

- *Is the directive clear and well understood?*
- *Do you have any suggestions on ways to address the directive?*

# FERC Order 822

- *73. Therefore, pursuant to section 215(d)(5) of the FPA, we direct NERC to develop a modification to provide the needed clarity, **within one year of the effective date of this Final Rule**. We agree with NERC and other commenters that a suitable means to address our concern is to modify the Low Impact External Routable Connectivity definition consistent with the commentary in the Guidelines and Technical Basis section of CIP-003-6.*

# FERC Order 822 Paragraph 73

- *Is the directive clear and well understood?*
- *Do you have any suggestions on ways to address the directive?*

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Project 2016-02 – Modifications to CIP Standards

Version 5 Transition Advisory Group Issues

RELIABILITY | ACCOUNTABILITY




# 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

# 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

# V5 TAG Issue - Cyber Asset and BES Cyber Asset Definitions

- *Is the issue clear and well understood?*
- *Do you have any suggestions on ways to address the issue?*

# 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."

# V5 TAG Issue - Network and Externally Accessible Devices

- *Is the issue clear and well understood?*
- *Do you have any suggestions on ways to address the issue?*

# 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

# V5 TAG Issue – TO Control Centers

- *Is the issue clear and well understood?*
- *Do you have any suggestions on ways to address the issue?*

# 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

# V5 TAG Issue – Virtualization

- *Is the issue clear and well understood?*
- *Do you have any suggestions on ways to address the issue?*

# Timeline

- March 23-April 21 – SAR posted for 30-day informal comment period
- April 20, 2016 – Request appointment of new SDT members
- May 24-26, 2016 – Initial SDT face-to-face meeting in Atlanta

# Information

- Senior Standards Developer, Steve Crutchfield
  - Email at stephen.crutchfield@nerc.net
  - Telephone: 609-651-9455
- Senior Standards Developer, Al McMeekin, P.E.
  - Email at al.mcmeekin@nerc.net
  - Telephone: 404-446-9675

# Questions