NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Supply Chain Cybersecurity Risk Management Standards

Technical Conference

November 10, 2016

RELIABILITY | ACCOUNTABILITY

Agenda

- Opening remarks
- Review conference objectives and ground rules
- Standards project overview
- Discuss draft Standard and technical guidance
  - Panel
- Recap
- Next Steps

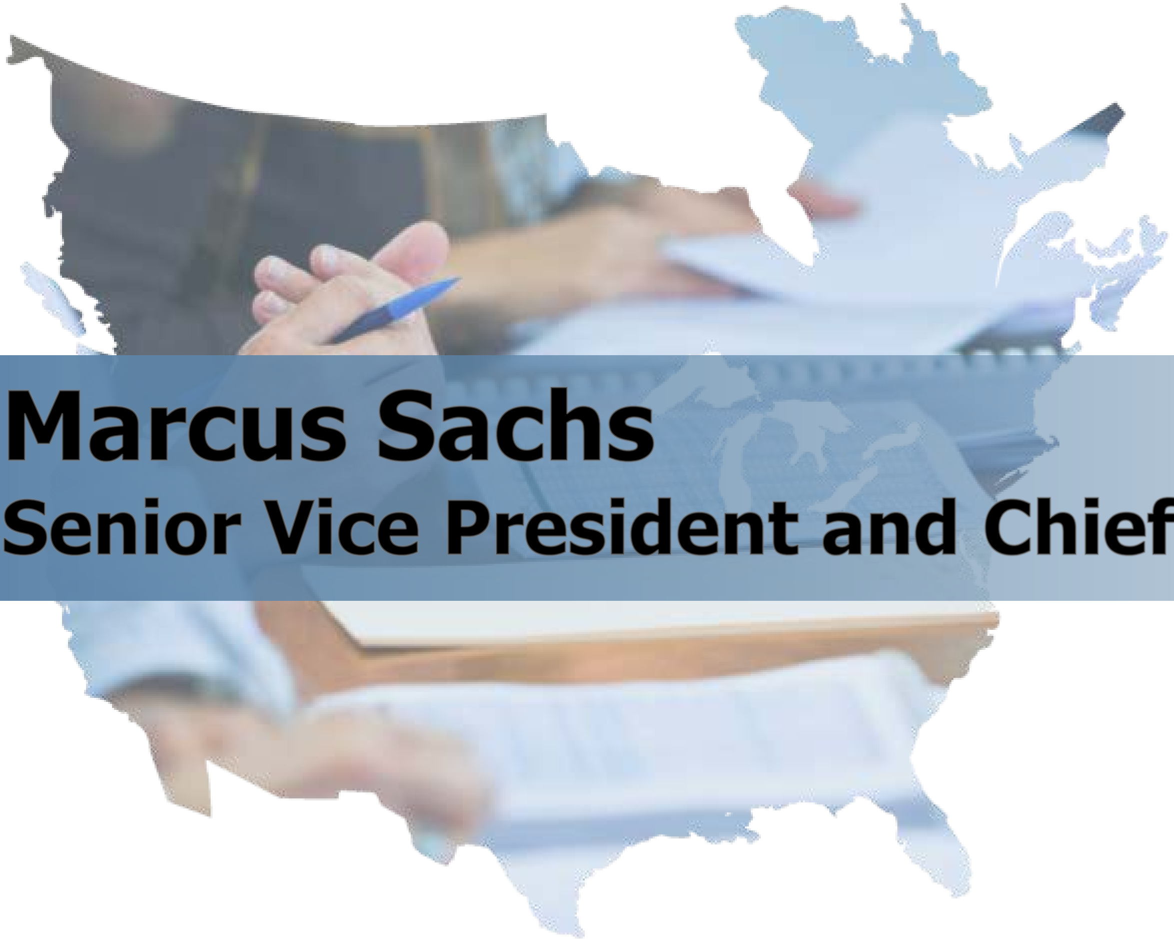
NERC Antitrust Compliance Guidelines and Public Announcement

- 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. It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.
- Participants are reminded that this meeting is public. Notice of the meeting was posted on the NERC website and widely distributed. Participants should keep in mind that the audience may include members of the press and representatives of various governmental authorities, in addition to the expected participation by industry stakeholders.

Introductory Remarks

Gerry Cauley

President and Chief Executive Officer



Marcus Sachs

Senior Vice President and Chief Security Officer

Objectives and Ground Rules

Conference Objectives

- Focus on providing early input to the standard drafting team (SDT) on draft Standard Requirements, technical guidance, and implementation guidance for addressing FERC Order No. 829
- Inform stakeholders on the project plan

Ground Rules

- Active facilitation
- Learn together, while staying true to Order No. 829 and needs of SDT
- Safe place to discuss issues and exchange ideas
- Focused discussion/questions
- Role of panel

Project 2016-03 Overview

Standard Drafting Team

Name	Entity
Corey Sellers (Chair)	Southern Company
JoAnn Murphy (Vice Chair)	PJM Interconnection, LLC
Christina Alston	Georgia Transmission Corp.
James W. Chuber	Duke Energy
Norm Dang	IESO of Ontario
Chris Evans	Southwest Power Pool
Brian Gatus	Southern California Edison Company
Brian Gayle	Dominion Resources Services, Inc.
Rusty Griffin	CPS Energy
Skip Peeples	Salt River Project
Jason Witt	East Kentucky Power Cooperative

FERC Order No. 829

[the Commission directs] that NERC, pursuant to section 215(d)(5) of the FPA, develop a forward-looking, objective-driven new or modified Reliability Standard to ***require each affected entity to develop and implement a plan that includes security controls for supply chain management*** *for industrial control system hardware, software, and services associated with bulk electric system operations. (P 43)*

- July 2016

Filing Deadline

- *[the Commission directs] NERC to submit the new or modified Reliability Standard within one year of the effective date of this Final Rule. (P 44)*

- Standard must be filed by September 27, 2017

Standard Authorization Request (SAR)

The SDT shall address each of the Order No. 829 directives. The Reliability Standard(s) developed or revised in the project will require applicable entities to develop and implement a plan that addresses, at a minimum, the following four specific objectives as they relate to supply chain cybersecurity of the BES (P 45):

1. *Software integrity and authenticity;*
2. *Vendor remote access;*
3. *Information system planning; and*
4. *Vendor risk management and procurement controls.*

SAR is posted for comment through November 18, 2016

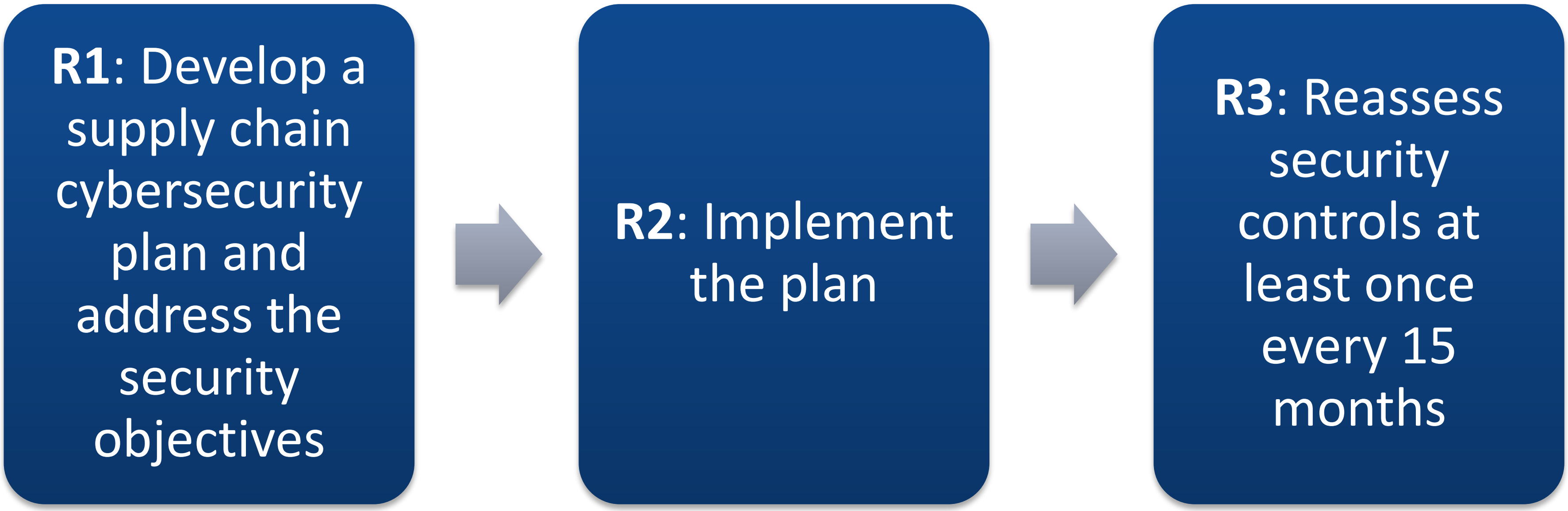
Other Guidance in Order No. 829

- *Responsible entities should be required to achieve these four objectives but have the flexibility as to how to reach the objective… (P 45)*

- *…any action taken by NERC in response to the Commission's directive to address the supply chain-related reliability gap should respect 'section 215 jurisdiction by only addressing the obligations of responsible entities' (P 21)*

- *…the new or modified Reliability Standard may allow a responsible entity to meet the security objectives discussed below by having a plan to apply different controls based on the criticality of different assets (P 44)*

Structure of Draft CIP-013-1



R1: Develop a supply chain cybersecurity plan and address the security objectives

R2: Implement the plan

R3: Reassess security controls at least once every 15 months

- Draft CIP-013-1 contains results-based Requirements addressing the directives of Order No. 829
- The SDT intends to support the results-based Requirements with **Guidelines and Technical Basis** and **Implementation Guidance**

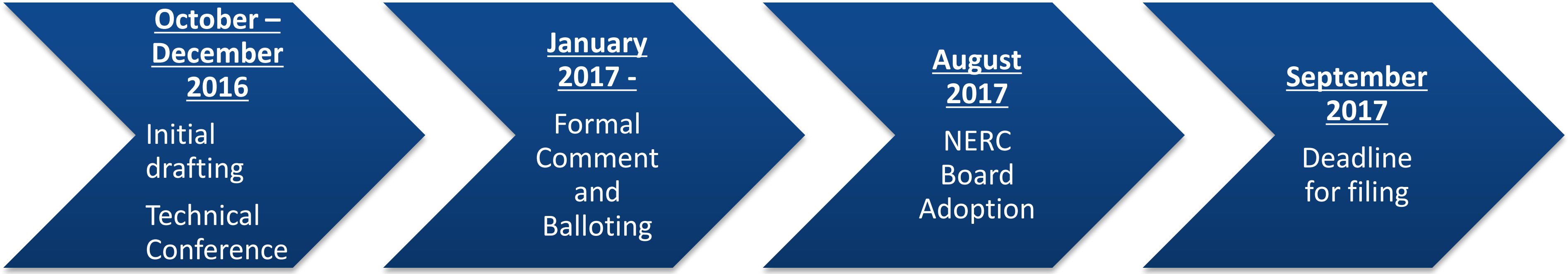
Guidelines and Technical Basis

- Informational section of the Standard written by the SDT containing:
  - Technical basis for Requirements
  - Guidelines for meeting the Requirements
- Revised by the SDT with stakeholder input during the standards development process

Implementation Guidance

- Implementation Guidance assists Registered Entities with implementing a Standard
- Provides examples or approaches to illustrate compliance
  - See approved Compliance Guidance Policy
  - Electric Reliability Organization (ERO) endorsed guidance clarifies compliance expectations
- NERC and the SDT intend to seek ERO endorsement in parallel with Standard development

Project Timeline



October – December 2016

Initial drafting

Technical Conference

January 2017 -

Formal Comment and Balloting

August 2017

NERC Board Adoption

September 2017

Deadline for filing

Discussion

Discussion of Draft CIP-013-1

Purpose

To mitigate risks of cybersecurity incidents affecting the reliable operation of the Bulk Electric System (BES) by implementing security controls in the supply chain for BES Cyber Assets and computing and networking services that impact BES operations.

Applicable Entities

Same as CIP-003-6 and other cybersecurity Reliability Standards

- Balancing Authority
- Distribution Provider*
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator

*Distribution Provider owning an applicable underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system, Remedial Action Scheme, Protection System, and Blackstart Cranking Path

Applicable Facilities

Same as CIP-003-6 and other cybersecurity Reliability Standards

- All BES Facilities
- Distribution Provider's applicable facilities*
- Exemptions
  - Cyber Assets associated with communications between discrete Electronic Security Perimeters (ESPs)
  - Cyber Assets covered under nuclear regulatory authorities (U.S. and Canada)

*Distribution Provider's applicable underfrequency Load shedding or undervoltage Load shedding system, Remedial Action Scheme, Protection System, or Blackstart Cranking Path

Requirement R1

Draft Standard

Requirement R1 requires entities to develop supply chain cybersecurity risk management plan addressing the objectives for BES Cyber Systems, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets.

Order

Require plans that include security controls for supply chain management for industrial control system hardware, software, and services associated with bulk electric system operations. *(P 43)*

Requirement R1

Draft Standard

Requirement R1 requires entities to develop supply chain cybersecurity risk management plan addressing the objectives for BES Cyber Systems, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets.

Order

Require plans that include security controls for supply chain management for industrial control system hardware, software, and services associated with bulk electric system operations. *(P 43)*

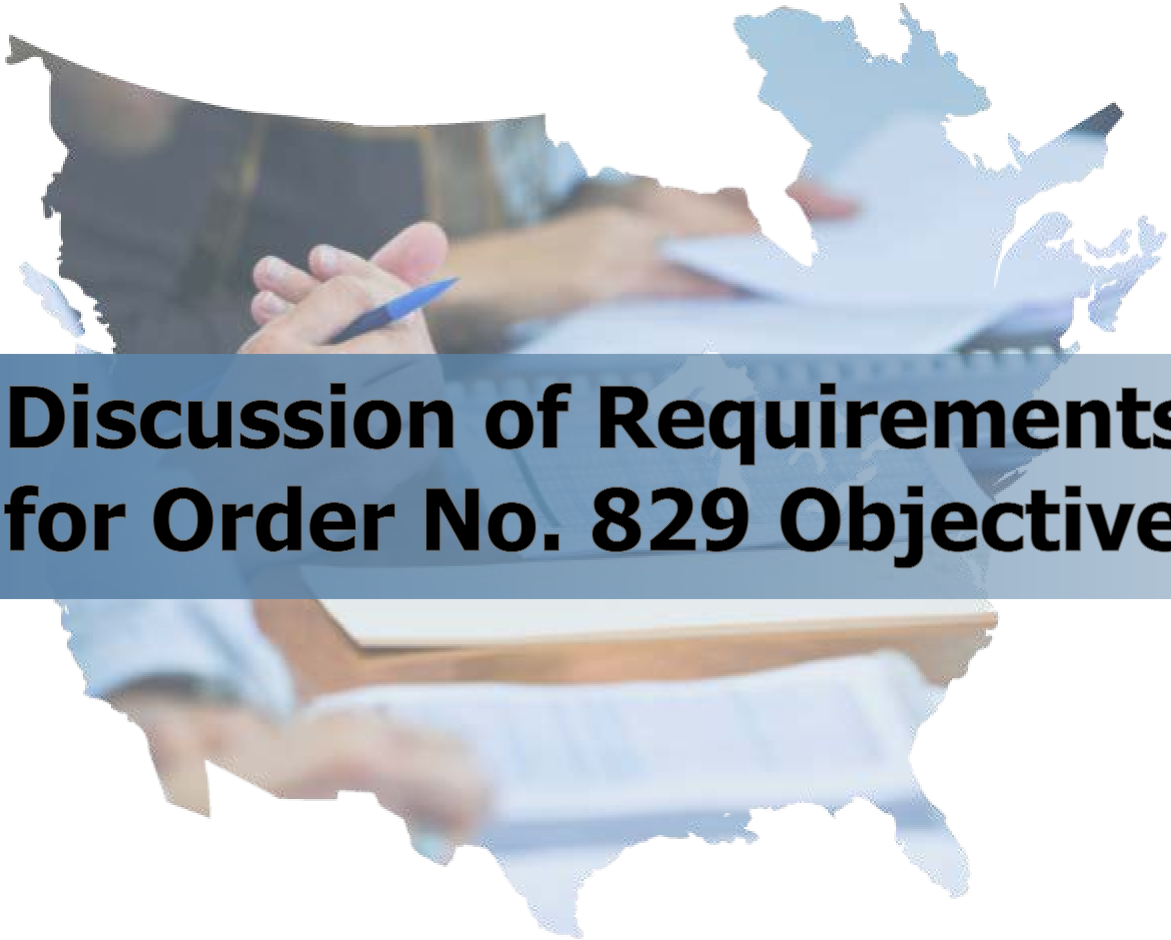
Technical Guidance for R1

Draft Guidance

- Generally identifies approaches that an entity could consider in developing a risk-based plan
  - Criticality of assets (**High**, **Medium**, and **Low** BES Cyber Systems)
  - Based on the entity's vendor/supplier considerations

Order

- Plans may apply different controls based on the criticality of different assets (P 44)
- Entities should have the flexibility as to how to reach the objectives (P 45)



Discussion of Requirements and Controls for Order No. 829 Objectives

Introduction of Panelists

- Paul Ackerman, Exelon
- Jeff Craigo, ReliabilityFirst
- Joe Doetzl, ABB
- John Galloway, Ph.D., ISO New England
- Rob Koziy, OSI International
- Steve McElwee, PJM Interconnection
- Scott Mix, NERC
- Jess Smith, Ph.D., Schweitzer Engineering Laboratories

1: Software Integrity and Authenticity

Draft Standard

Requirement R1 Part 1.1. specifies that plans must include software integrity and authenticity controls that provide for verification of the following prior to installation:

1.1.1. The identity of the publisher for software and firmware, and any upgrades and patches to software and firmware;

1.1.2. The integrity of software and firmware upgrades and patches.

Order

- Plans must address verification of (P 48):
  - Identity of the software publisher for all software and patches intended for use on BES Cyber Systems
  - Integrity of the software and patches before they are installed in the BES Cyber System environment

Technical Guidance for Objective 1

Examples of controls for **Software Integrity and Authenticity**

- Procedures to ensure patches are from the original source
- Server side encryption keys with validation processes
- Procedures for verifying digital signatures and certificates
- Require use of digital fingerprints and checksums

2: Vendor Remote Access

Draft Standard

Requirement R1 Part 1.2. specifies that plans must include remote access controls that provide for :

1.2.1. Controlling and **(1.2.2)** monitoring third-party initiated remote access including machine-to-machine;

1.2.3. Detecting and responding to unauthorized third-party remote access activity.

Order

- Plans must address:
  - Logging and controlling all third-party initiated remote access including machine-to-machine (P 51)
  - controls to provide the ability to rapidly disable remote access sessions in the event of a system breach (P 52)

Technical Guidance for Objective 2

Examples of controls for **Vendor Remote Access**

- Operator-controlled, time-limited access
- Logging and review procedures
- System alerts (e.g. failed log-in)
- Jump hosts for access to protected networks
- Changing default passwords
- Monitoring and acting on advisories
- Contract terms to support controls

3: Information System Planning

Draft Standard

Requirement R1 Part 1.3. specifies that plans must include Information system planning controls that:

1.3.1. Assess risks that may be introduced by a third-party

1.3.2. Evaluate methods to address identified third-party risk

Implementation of controls may be added by the SDT to the Requirement, or addressed in separate Requirement in the Standard

Order

- The Standard must address (P 56)
  - Identification and documentation of risks in information system planning
  - Consideration of risks and the available options for hardening the responsible entity’s information system and minimizing the attack surface.

Technical Guidance for Objective 3

Examples of controls for **Information System Planning**

- Screening criteria to determine high-risk systems or changes
- Processes to assess third-party risks in planning including
    - Gathering and review of information on vendor security processes
    - Engaging vendors in testing of potential vulnerabilities
    - Use of available tools for establishing vendor risk baseline
- New system design processes to incorporate layered protections, security policy, architecture, and controls
- Planning controls to identify and replace unsupported system components, or authorize continued use for specific purposes
- Processes for coordination and approval involving appropriate IT security, supply chain, and legal personnel
- Procurement controls including standard contract provisions

4: Vendor Risk Management and Procurement Controls

Draft Standard

Requirement R1 Part 1.4. specifies that plans must include procurement controls to verify security controls used by vendors and suppliers. The controls must provide for:

- **1.4.1.** Notification of security events that could impact the entity
- **1.4.2.** Notification when employee access should be removed
- **1.4.3.** Disclosure of known vulnerabilities that could impact the entity
- **1.4.4.** Coordination of response to vendor-related cybersecurity incidents

Order

- The Standard must address the provision and verification of the above-listed security concepts in future contracts (P 59)

Technical Guidance for Objective 4

Examples of controls for **Vendor Risk Management**

- Incorporate risk-assessment information in Requests for Proposals (RFPs)
- Establish procurement review teams that include CIP personnel
- Develop contract terms addressing each topic and methods for monitor performance. Consider requesting
  - Relevant testing results or other product details
  - Cooperation with periodic security reviews
  - Restrict use of responsible entity name in vendor public information
- Vendor policies may not support notifying entities of vulnerabilities **prior to the vendor determining mitigation**

Requirement R2

Draft Standard

- **Requirement R2** requires entities to implement supply chain cybersecurity risk management plan
  - Implementation of the plan does not require renegotiation of existing contracts

Order

- Require plans that include security controls for supply chain management (P 43)
  - The Standard should not require the abrogation or re-negotiation of currently-effective contracts with vendors or suppliers (P 36)

Requirement R3

Draft Standard

- **Requirement R3** requires entities to review and obtain CIP Senior Manager (or delegate) approval of controls in the plan at least once every 15 months
  - Review must include consideration of new risks, mitigations, and changes

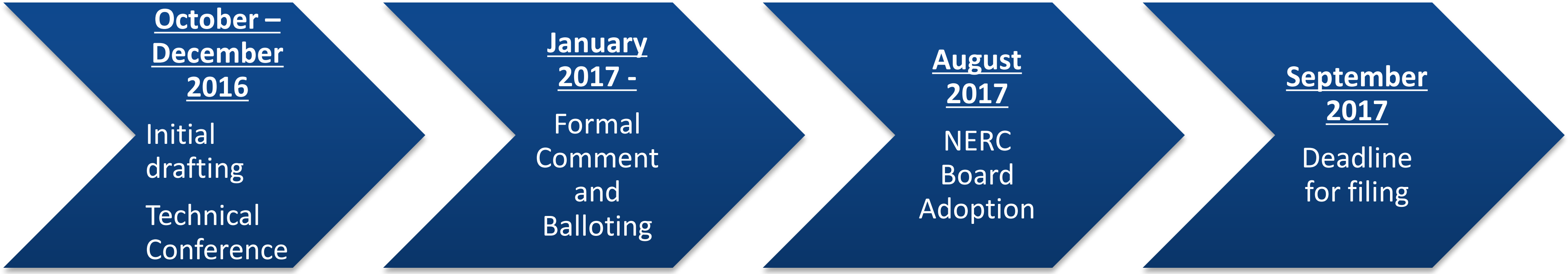
Order

- Require periodic reassessment with or similar to CIP-003-6 Requirement R1 at least every 15 months (P 46)
  - Review should consider guidance from NERC, U.S. Department of Homeland Security, and other authorities (P 47)

Recap Themes

Next Steps

Project Timeline



October – December 2016

Initial drafting

Technical Conference

January 2017 -

Formal Comment and Balloting

August 2017

NERC Board Adoption

September 2017

Deadline for filing

- SDT meeting to revise drafts: November 29 – December 1, 2016
    - Meeting information is available on the NERC Calendar

Wrap-up

Reference Slides

Contact Information

- Refer to the Project 2016-03 page for more information
- Email mark.olson@nerc.net to join the email list
- Corey Sellers, Southern Company, SDT Chair
  - Email at mcseller@southernco.com
- JoAnn Murphy, PJM Interconnection, SDT Vice Chair
  - Email at joann.murphy@pjm.com

Definitions

BES Cyber System

One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.

Definitions

BES Cyber Asset

A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. (A Cyber Asset is not a BES Cyber Asset if, for 30 consecutive calendar days or less, it is directly connected to a network within an ESP, a Cyber Asset within an ESP, or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.)

Definitions

Protected Cyber Assets

One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP. A Cyber Asset is not a Protected Cyber Asset if, for 30 consecutive calendar days or less, it is connected either to a Cyber Asset within the ESP or to the network within the ESP, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Definitions

Electronic Access Control or Monitoring Systems

Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems.

Physical Access Control Systems

Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.