RELIABILITY & SECURITY

Workshop - Portland, Oregon

October 29–30, 2024

Project 2016-02: Early Adoption and Transition

October 30, 2024

Morgan King, Senior Technical Advisor, Cybersecurity, WECC

Scott Klauminzer, CIP Program Manager, TPWR

Lenin Maran, Manager, EMS: Systems, Security and Compliance, SMUD

Tom Williams, Entity Monitoring Manager, WECC

Introductions

Morgan King

Senior Technical Advisor, Cyber Security (WECC)

Scott Klauminzer

Critical Infrastructure Protection Program Manager, Tacoma Public Utilities (TPWR)

Lenin Maran

EMS Manager: Systems, Security, and Compliance (SMUD)

Tom Williams

Manager, Entity Monitoring (WECC)

What You Will Learn and Why It Matters

In this session, we will cover some key areas to launch you on your transition to new versions of most CIP Standards.

- Background of Project 2016-02
- Status on FERC approval and timeline
- Early adoption
- Backward compatibility

It is a challenge for standards to keep up with the pace of technology change; the changes in Project 2016-02 will give entities more flexibility in their technical implementation of CIP controls and, in a sense, "future proof" the CIP Standards.

- New and modified definitions in the NERC Glossary of Terms
- Transition from network perimeter to security perimeter
- Development of Implementation Guidance
- Possibility of Small Group Advisory Sessions

Background

The Version 5 Transition Advisory Group (V5 TAG) transferred issues to the Version 5 SDT that were identified during the industry transition to implementation of the Version 5 CIP Standards. Specifically, the issues that the SDT will address are:

- Cyber Asset and BES Cyber Asset Definition
- Network and Externally Accessible Devices
- Transmission Owner (TO) Control Centers Performing Transmission Operator (TOP) Obligations
- Virtualization

On January 21, 2016, FERC issued Order No. 822 Revised Critical Infrastructure Protection Reliability Standards. In this order, FERC approved revisions to version 5 of the CIP standards and also directed that NERC address each of the Order 822 directives by developing modifications to requirements in CIP standards and the definition of Low Impact External Routable Connectivity (LERC), or the SDT shall develop an equally efficient and effective alternative. To address concerns identified in Order 822, the Commission directed the following:

- 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.
- 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).
- Develop a modification to provide the needed clarity, within one year of the effective date of this Final Rule, to the LERC definition consistent with the commentary in the Guidelines and Technical Basis section of CIP-003-6.

Project 2016-02 Modifications to CIP Standards

What main constraints and limitations does Project 2016-02 seek to address?

New Versions of Standards

CIP-002-7

CIP-003-10

CIP-004-8

CIP-005-8

CIP-006-7

CIP-007-7

CIP-008-7

CIP-009-7

CIP-010-5

CIP-011-4

CIP-013-3

Project 2016-02 began more than eight years ago. What have been the main challenges?

May 9, 2024: approved by NERC.

July 10, 2024: filed with FERC.

Entities may choose to adopt the revised Standards early. What does early adoption mean? Can I pick the date?

Early Adoption

Early Adoption Date
Option 1: First day of the first calendar quarter that is six (6) months after the effective date of the applicable governmental authority's order approving the Revised CIP Standards and Definitions
Option 2: First day of the first calendar quarter that is twelve (12) months after the effective date of the applicable governmental authority's order approving the Revised CIP Standards and Definitions
Option 3: First day of the first calendar quarter that is eighteen (18) months after the effective date of the applicable governmental authority's order approving the Revised CIP Standards and Definitions

Responsible Entities must comply with applicable Requested CIP Retired Standards until their selected Early Adoption Date. All Responsible Entities, regardless of whether or not they selected an Early Adoption Date, must comply with the Revised CIP Standards and Definitions by the Effective Date.

Implementation Plan — Project 2016-02 Modifications to CIP Standards

Are the revised Standards backward compatible?

Will I need to virtualize?

Backward Compatibility

- Entities need not virtualize
- Compliance implementation will change for CIP-010-5, whether entities virtualize or not

> As the vendors of our systems incorporate more and more virtualization and advanced technology, it is challenging the way we characterize the Critical Infrastructure Protection (CIP) standards' objectives and how we develop technical requirements. Use of virtualization and advanced technology can provide benefits for implementing both operational and security enhancements to a system. The goal is to require technology-enforced controls that meet security objectives as alternatives to the current prescriptive requirements like those requiring a physically structured architecture, without forcing the use of the new technology. The existing standards with their prescriptive language limit the ability to take full advantage of the new technologies. The Project 2016-02 Modifications to CIP Standards Standard Drafting Team (SDT) is modifying existing requirements and drafting new requirements to support virtualization capabilities. This leaves Responsible Entities with the option to maintain a non-virtualized environment and use backward compatibility to preserve current CIP investments and security postures.

Virtualization and Future Technologies — Project 2016-02 Standards Drafting Team: What's in it for me?

There are four new NERC defined terms? What are they and why do we need them?

New Term	Definition
Cyber System	One or more Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure.
Management Interface	An administrative interface that: • Controls the processes of initializing, deploying, and configuring Shared Cyber Infrastructure; • Is an autonomous subsystem that provides access to the console independently of the host system's CPU, firmware, and operating system; or • Configures an Electronic Access Point.
Shared Cyber Infrastructure (SCI)	One or more programmable electronic devices, including the software that shares the devices' resources, that: • Hosts one or more Virtual Cyber Assets (VCA) included in a BES Cyber Systems (BCS) or their associated Electronic Access Control or Monitoring Systems (EACMS) or Physical Access Control Systems (PACS); and hosts one or more VCAs that are not included in, or associated with, BCS of the same impact categorization; or • Provides storage resources required for system functionality of one or more Cyber Assets or VCAs included in a BCS or their associated EACMS or PACS; and also for one or more Cyber Assets or VCAs that are not included in, or associated with, BCS of the same impact categorization. SCI does not include the supported VCAs or Cyber Assets with which it shares its resources.
Virtual Cyber Asset (VCA)	A logical instance of an operating system or firmware, currently executing on a virtual machine hosted on a BES Cyber Asset; Electronic Access Control or Monitoring System; Physical Access Control System; Protected Cyber Asset; or Shared Cyber Infrastructure (SCI). Virtual Cyber Assets (VCAs) do not include: • Logical instances that are being actively remediated in an environment that isolates routable connectivity from BES Cyber Systems; • Dormant file-based images that contain operating systems or firmware; or • SCI or Cyber Assets that host VCAs. Application containers are considered software of VCAs or Cyber Assets.

Are the definitions for Electronic Security Perimeter, Interactive Remote Access, and Intermediate System going to change?

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised Definition
Electronic Security Perimeter (ESP)	The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol.	The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol; or a logical boundary defined by one or more Electronic Access Points.
Interactive Remote Access (IRA)	User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.	User-initiated electronic access by a person using a bi-directional routable protocol: • To a Cyber System protected by an Electronic Security Perimeter(s) (ESP); • That is converted by the responsible entity to a non-routable protocol that allows access to a Cyber System; or • To a Management Interface. Interactive Remote Access does not include: • Communication that originates from a Cyber System protected by any of the Responsible Entity's ESPs; or • System-to-system process communication.
Intermediate System	A Cyber Asset or collection of Cyber Assets performing access control to restrict Interactive Remote Access to only authorized users. The Intermediate System must not be located inside the Electronic Security Perimeter.	One or more Electronic Access Control or Monitoring Systems that are used to restrict Interactive Remote Access to only authorized users.

Changes in CIP-005-8 allow more flexibility for virtual networks and software-defined networks (SDN). What is SDN? Could you share some perspective on what this change could mean in practice?

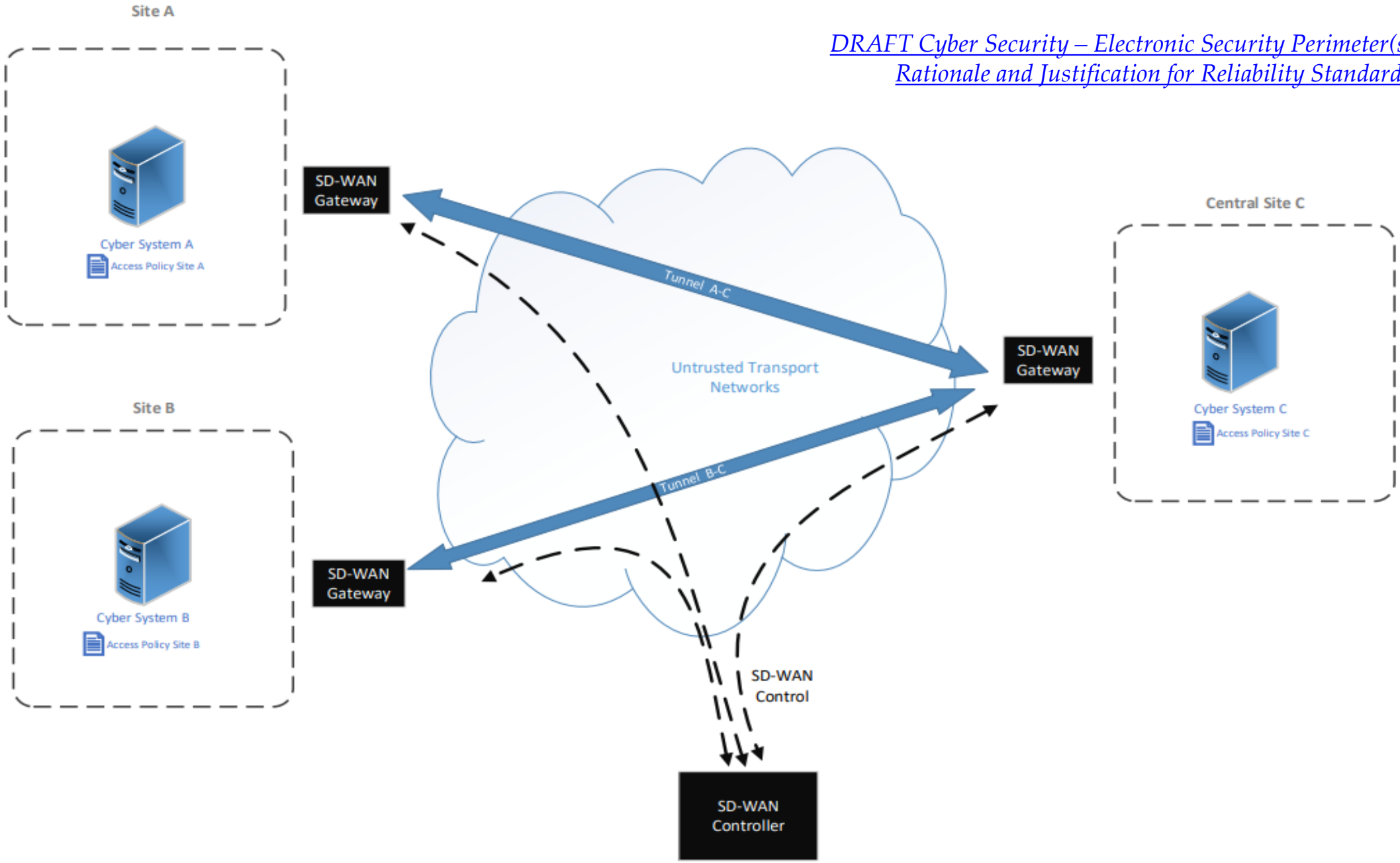


Figure 2 Typical SD-WAN

What are affinity rules in virtualization and why are they important for CIP?

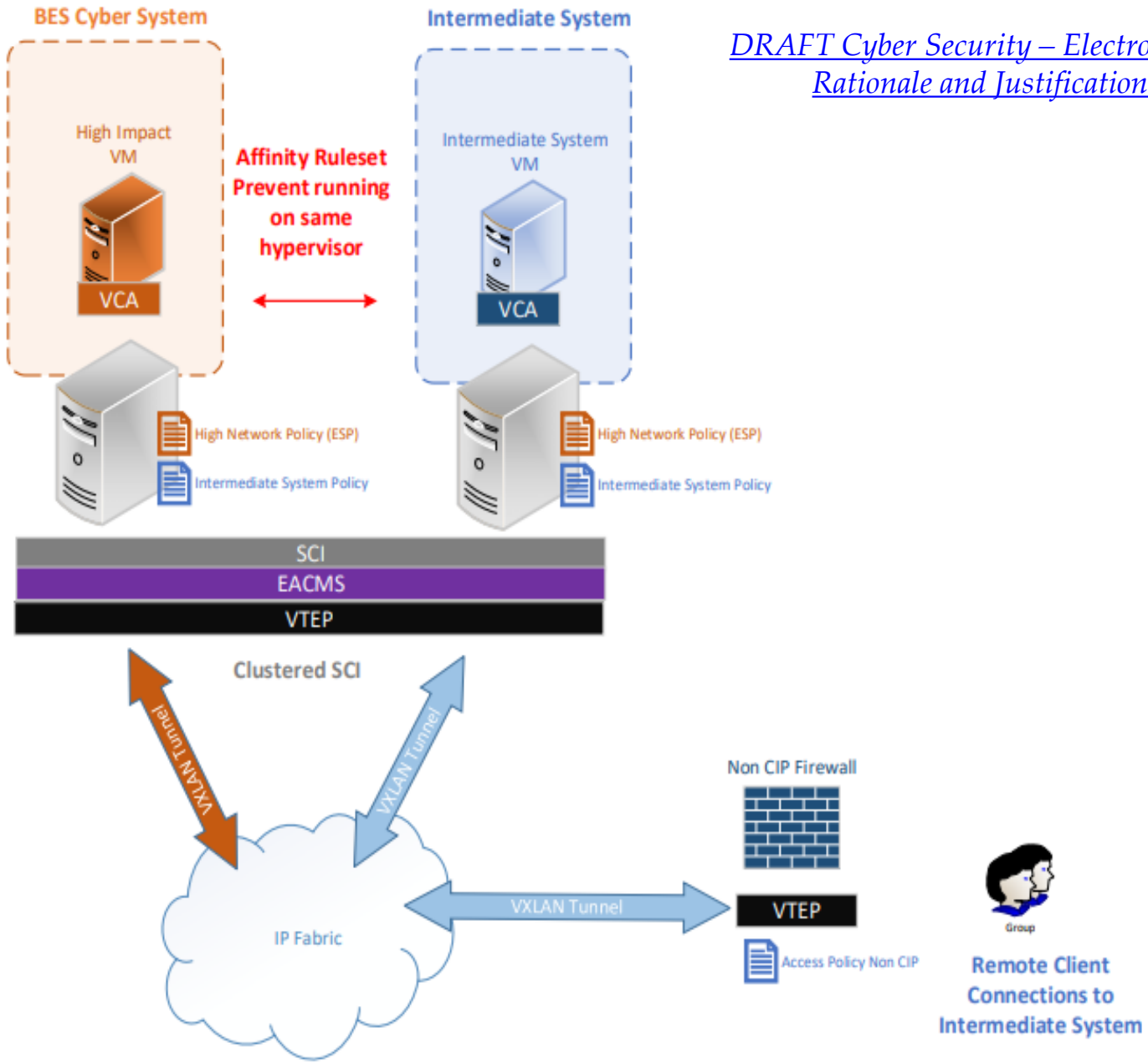


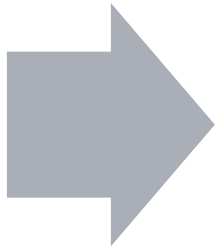
Figure 6 Affinity Rules - Intermediate System does not share CPU or share memory with BES Cyber Systems

What is the focus of the Implementation Guidance that WICF is writing? Why not a practice guide?

Implementation Guidance

- A dozen members from WICF, WECC, NERC, and the Drafting Team are writing Implementation Guidance for CIP-010-5 R1, Parts 1.1 and 1.4.
- The team will focus on multiple scenarios covering automation and virtualization.

Release to WICF and Drafting Team for review and comment



Submit to ERO Regions and NERC for endorsement

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Pre-Qualified Organizations for Submitting Implementation Guidance

As of June 18, 2020

Examples for proposed Implementation Guidance must be vetted through one of the following pre-qualified organizations prior to being submitted to the ERO Enterprise for endorsement. In order to become pre-qualified and be able to propose Implementation Guidance, an organization must submit a request to the Compliance & Certification Committee. Below is the current list of pre-qualified organizations:

1. American Public Power Association (APPA)
2. Canadian Electricity Association (CEA)
3. Edison Electric Institute (EEI)
4. Electricity Consumers Resource Council (ELCON)
5. Electric Power Supply Association (EPSA)
6. EnergySec
7. ISO/RTO Council
8. Large Public Power Council (LPPC)
9. National Association of Regulatory Utility Commissioners (NARUC)
10. National Rural Electric Cooperative Association (NRECA)
11. North American Generator Forum (NAGF)
12. North American Transmission Forum (NATF)
13. Northwest Public Power Association (NWPPA)
14. Nuclear Energy Institute (NEI)
15. Transmission Access Policy Study Group (TAPS)
16. Western Interconnection Compliance Forum (WICF)
17. NERC Reliability and Security Technical Committee (RSTC)
18. Regional Entity Stakeholder Committees

ERO Enterprise-Endorsed Implementation Guidance (24)

CIP (13)

- CIP-013 Using Independent Assessments of Vendors (NATF)
- CIP-013 Supply Chain Risk Management Plans (NATF)
- CIP-004-7 R6 and CIP-011-3 R1 - Cloud Solutions for BCSI (RSTC)
- CIP-012-1 Communications Between Control Centers (2016-02 SDT)
- CIP-013-1 Supply Chain Risk Management Plans (NATF)
- CIP-014-2, R5 Developing and Implementing Physical Security Plans (NATF)
- CIP-002-5.1a R1 Shared Ownership of BES Facilities (CIPC)
- CIP-014-2 R4 Evaluating Potential Physical Security Attack (NATF)
- CIP-010-3 R1.6 Software Integrity and Authenticity (NATF)
- CIP-004-6 R3 - NGOP Employee Access to TO Sites (CIPC)
- CIP-013-1 Supply Chain Risk Management Plans (2016-03 SDT)
- CIP-014-2, R1 Transmission System Risk Assessment (NATF)
- CIP-002-5.1 R1 Identify and Categorize BES Cyber Systems and Cyber Assets (MRO SC)

FAC (2)

PRC (5)

TOP (3)

TPL (1)

NERC One-Stop Shop — Compliance Guidance

What are Small Group Advisory Sessions? How could they be helpful for entities?

WECC

Electric Reliability and Security for the West

www.wecc.org