NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Join: slido.com
#2016-02-D1a

Project 2016-02

Modification to CIP Standards Outreach
Draft 1

CIP SDT Members
February 2021

RELIABILITY | RESILIENCE | SECURITY

Administrative Items

Join: slido.com
#2016-02-D1a

- 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.

The CIP Standards Drafting Team

Join: slido.com
#2016-02-D1a

	Name	Entity
Co-chair	Jay Cribb	Southern Company
Co-chair	Matthew Hyatt	Georgia System Operations Corporation
Members	Jake Brown	ERCOT
	Norman Dang	Independent Electricity Systems Operator of Ontario
	Robert Garcia	SPP, Inc.
	Scott Klauminzer	Tacoma Public Utilities
	Sharon Koller	ATC, LLC
	Heather Morgan	EDP Renewables
	Mark Riley	Associated Electric Cooperative, Inc.

Opening Remarks

Join: slido.com #2016-02-D1a

- **Webinar Purpose:** High level overview of modifications for Project 2016-02 Modification to CIP Standards 60-day initial comment and ballot period
- **Initial Posting Duration:** January 22 – March 22, 2021
  - 60-day comment and ballot period
  - Individual ballot pools – join by February 19, 2021
  - Ballot period: March 12-22, 2021
- **Standards Affected:** CIP-002 through CIP-011, and CIP-013
  - Standards with Changes: CIP-005, CIP-007, and CIP-010
  - Conforming Changes: CIP-002, CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013

Opening Remarks

Join: slido.com #2016-02-D1a

- Informational Filing to FERC
  - “Pursuant to paragraph 5 of the Order Directing Informational Filings Regarding NERC Standard Drafting Projects,1 the North American Electric Reliability Corporation (“NERC”)2 hereby submits to the Federal Energy Regulatory Commission (“FERC” or the “Commission”) an informational filing regarding two active Critical Infrastructure Protection (“CIP”) standard development projects: (1) Project 2016-02 –Modifications to CIP Standards (“Project 2016-02”)…”
  - Project 2016-02 Modification to CIP Standards Timeline
    - Initial comment and ballot period: January 22 – March 22, 2021
    - Additional comment period: June – July 2021
    - Additional comment and ballot period: September – October 2021
    - Final Ballot: October 2021

Initial Survey

Providing Feedback

Ask anonymously at anytime!
Vote other's questions up/down
Answer Polls and Surveys

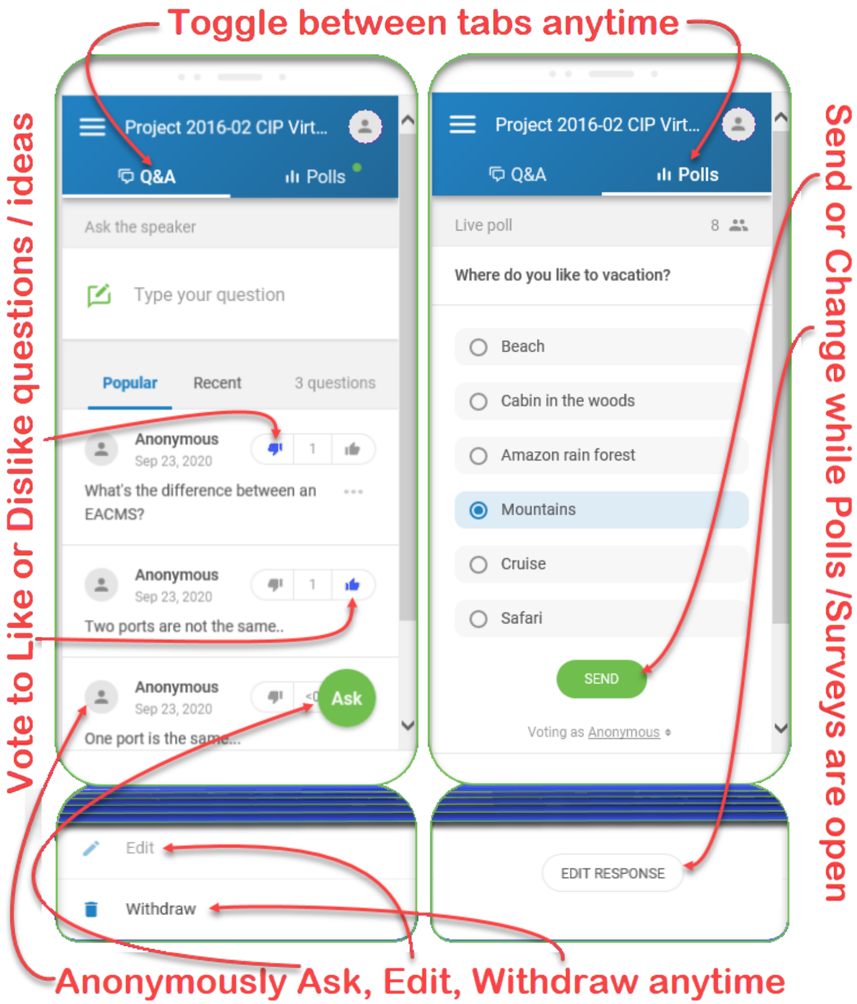
Join at
slido.com
#2016-02-D1a

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Slido Features and Navigation

Join: slido.com
#2016-02-D1a

Use the Mobile App or a Browser



Toggle between tabs anytime

Vote to Like or Dislike questions / ideas

Send or Change while Polls /Surveys are open

Anonymously Ask, Edit, Withdraw anytime

Project 2016-02 CIP Virt...
Q&A | Polls

Ask the speaker

Type your question

Popular | Recent | 3 questions

Anonymous
Sep 23, 2020
What's the difference between an EACMS?

Anonymous
Sep 23, 2020
Two ports are not the same..

Anonymous
Sep 23, 2020
One port is the same...

Ask

Edit

Withdraw

Project 2016-02 CIP Virt...
Q&A | Polls

Live poll 8

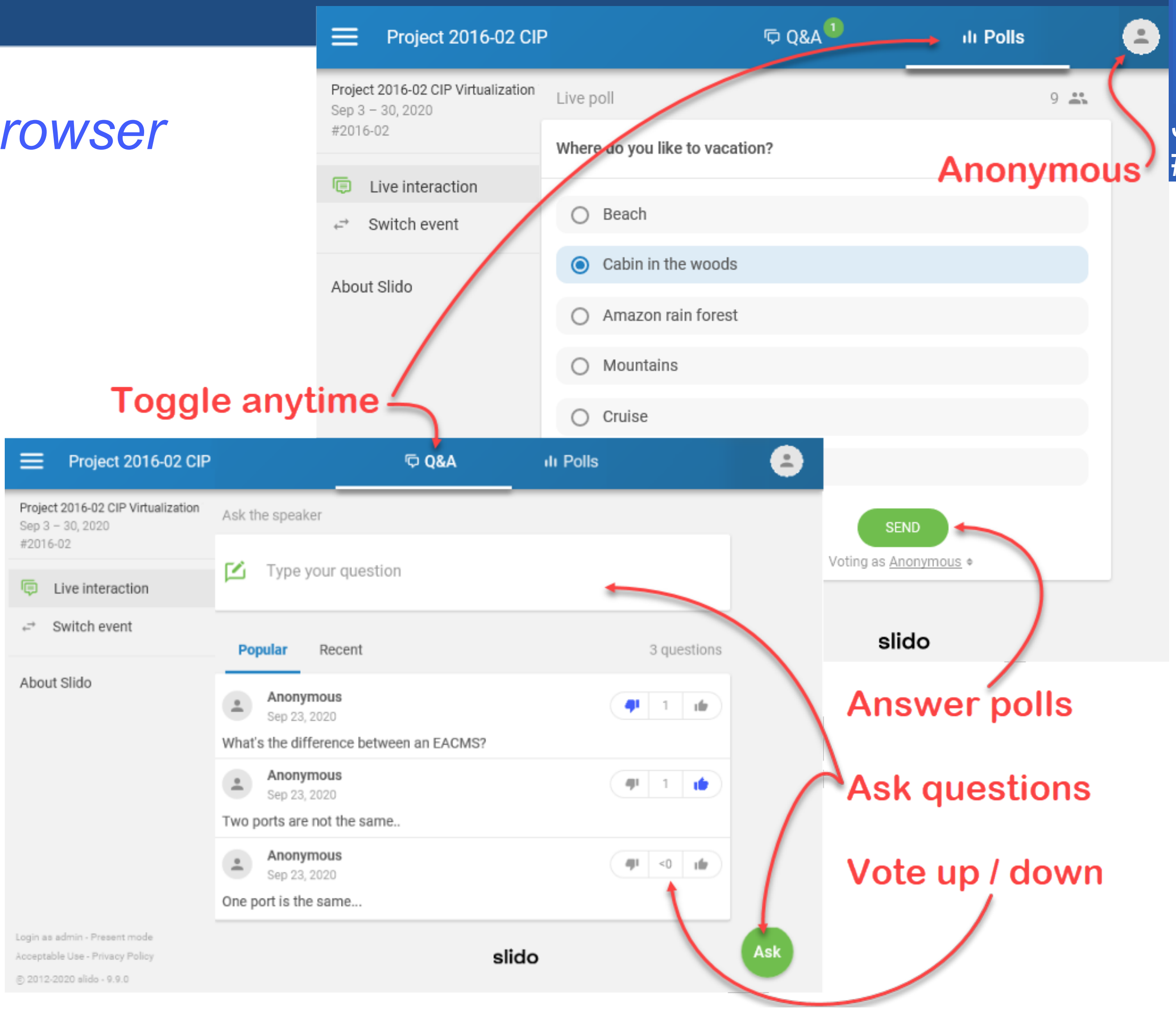
Where do you like to vacation?

○ Beach
○ Cabin in the woods
○ Amazon rain forest
● Mountains
○ Cruise
○ Safari

SEND

Voting as Anonymous

EDIT RESPONSE



Toggle anytime

Anonymous

Answer polls

Ask questions

Vote up / down

Project 2016-02 CIP
Q&A 1 | Polls

Project 2016-02 CIP Virtualization
Sep 3 – 30, 2020
#2016-02

Live interaction
Switch event
About Slido

Live poll 9

Where do you like to vacation?

○ Beach
● Cabin in the woods
○ Amazon rain forest
○ Mountains
○ Cruise

SEND

Voting as Anonymous

slido

Project 2016-02 CIP
Q&A | Polls

Project 2016-02 CIP Virtualization
Sep 3 – 30, 2020
#2016-02

Live interaction
Switch event
About Slido

Ask the speaker

Type your question

Popular | Recent | 3 questions

Anonymous
Sep 23, 2020
What's the difference between an EACMS?

Anonymous
Sep 23, 2020
Two ports are not the same..

Anonymous
Sep 23, 2020
One port is the same...

Login as admin · Present mode
Acceptable Use · Privacy Policy
© 2012-2020 slido · 9.9.0

slido

Ask

Webinar Agenda

Join: slido.com
#2016-02-D1a

- Overall webinar plan
- Scope of changes
- Key Concepts
  - Virtualization
  - Logical Isolation/Zero Trust
- ERC and IRA
- Technical Rationale “Lite”
  - High/Moderate/Minor level of change
- Resources
- Q&A

Scope of Changes from SAR

- V5TAG Items
  - Virtualization
    - "The CIP V5 standards do not specifically address virtualization. Because of the increasing use of virtualization in industrial control system environments, V5TAG asked that the SDT consider the CIP V5 standards and the associated definitions regarding permitted architecture and the security risks of virtualization technologies."
  - Clarification of ERC/IRA
    - "V5TAG recommends improving clarity within the concepts and requirements concerning Electronic Security Perimeters (ESP), External Routable Connectivity (ERC), and Interactive Remote Access (IRA) "
- CIP Exceptional Circumstances (CEC)
  - "…the SDT will review and address the CIP V5 requirements for CIP Exceptional Circumstances exceptions."
- Standard Template Conformity
  - Removal of Guidelines and Technical Basis (GTB) and Background sections to Technical Rationale documents.

Join: slido.com
#2016-02-D1a

Key Virtualization Concepts

A High Level Summary of What changed and Why

Key Concepts - Virtualization

Join: slido.com
#2016-02-D1a

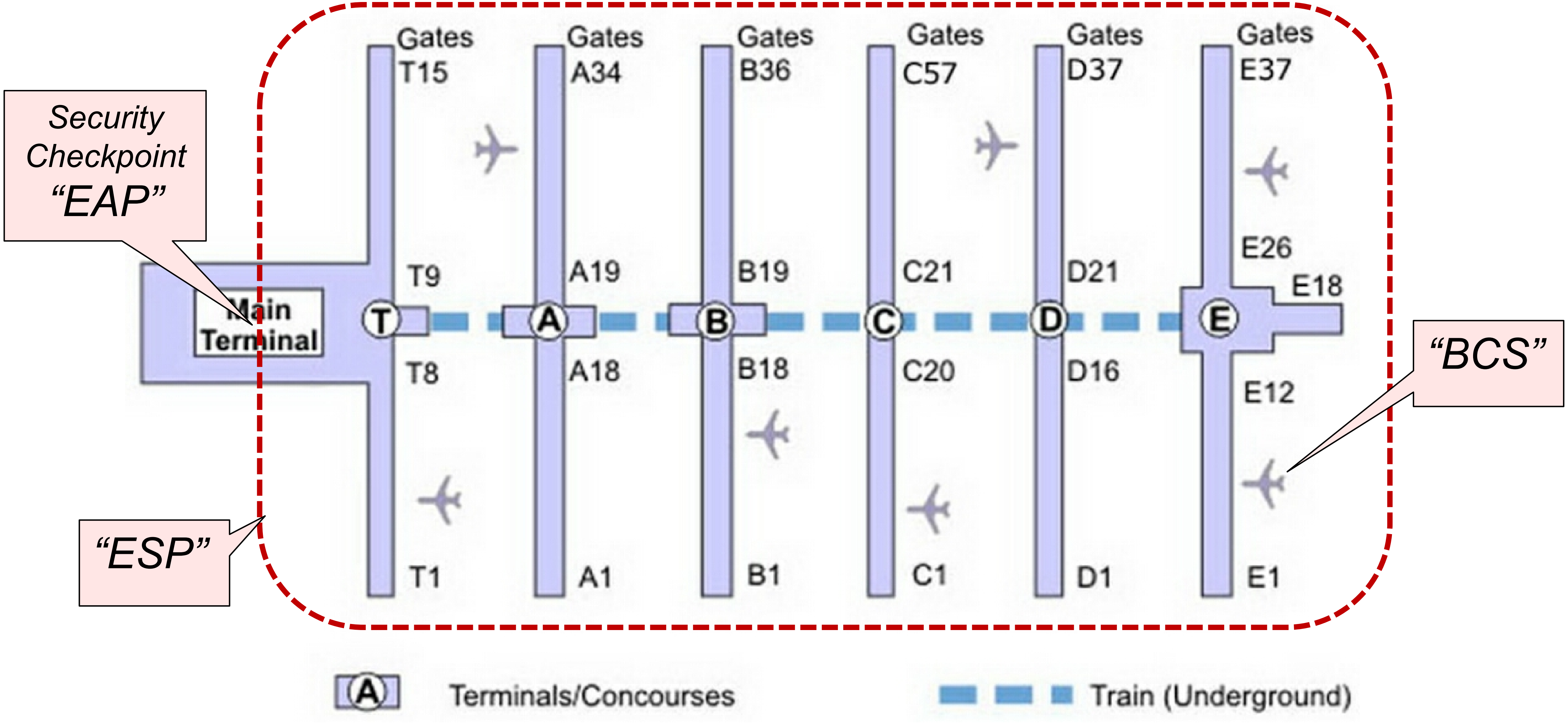
- Virtualization
  - Timing - Why now?
  - On-premise only (not off-premise cloud)
  - Virtual Cyber Asset (VCA) and Shared Cyber Infrastructure (SCI) to address Hardware/Software abstraction
  - Securing the Management Plane (Management Systems, Management Modules, Management Interfaces)
  - Standards Format – inclusion in current CIP standards vs. “dedicated virtualization standard”

Key Concepts – Logical Isolation

Join: slido.com
#2016-02-D1a

- Logical Isolation in CIP-005
  - A higher-level security objective
  - What does an ESP "do"?
    - It logically isolates a particular group of hosts; permitting only necessary inbound/outbound traffic and isolates those hosts from all other traffic from all other hosts.
    - ESP/EAP is ONE way to achieve that objective; but no longer the only way
  - CIP-005 no longer prescribes WHERE the network access decisions must be made.
    - Allows for other architectures that address cyber security risks

Logical Isolation & Zero Trust



Logical Isolation – Zero Trust

Join: slido.com
#2016-02-D1a

- Zero Trust Architecture
  - Mitigate dynamic network and lateral movement risks (ransomware, SolarWinds, etc.)
  - From NIST SP 800-207
    - Zero trust (ZT) is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources.
    - Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location.
    - Authentication and authorization (both subject and device) are discrete functions performed before a session to an enterprise resource is established.
  - “Policy not Topology”

Key Concepts - Definitions

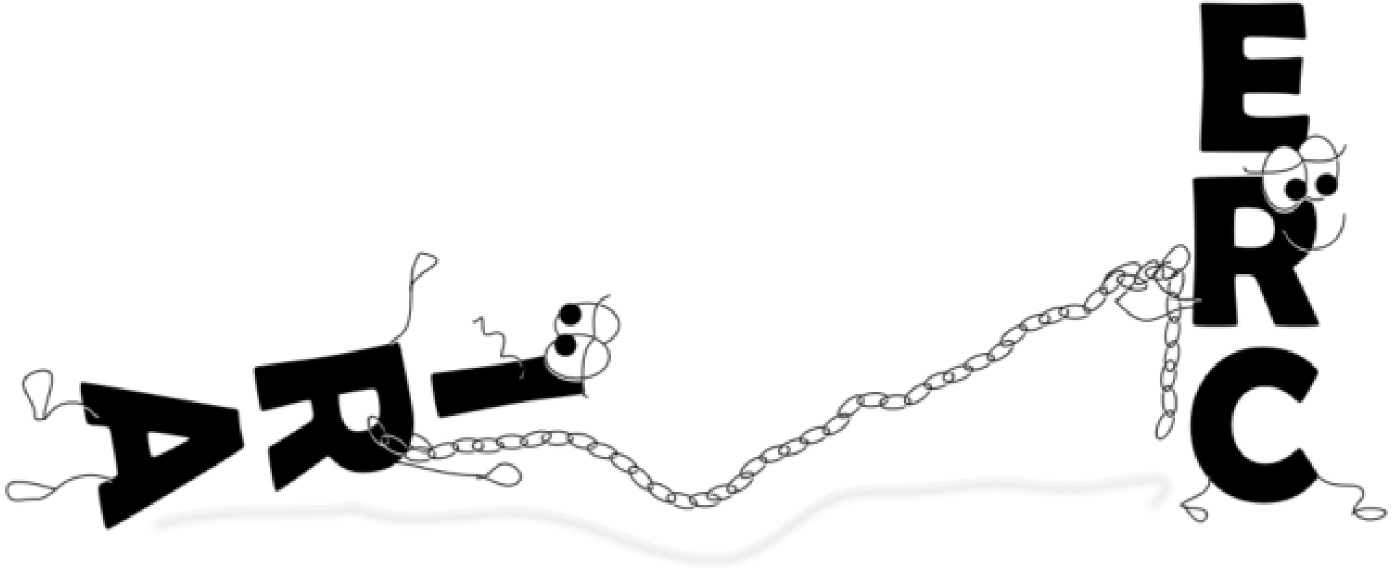
Join: slido.com
#2016-02-D1a

- Definitions
    - Modified to remove requirement scoping language
        - Examples:
            - CIP Senior Manager
            - Intermediate System
    - Adding Shared Cyber Infrastructure where BES Cyber System exists
    - Adding Virtual Cyber Asset where Cyber Asset exists
    - Enabling logical isolation by retiring ESP/EAP and removing ESP from other definitions

ERC/IRA Clarifications

Join: slido.com
#2016-02-D1a

- Clarification of ERC/IRA
  - "V5TAG recommends improving clarity within the concepts and requirements concerning Electronic Security Perimeters (ESP), External Routable Connectivity (ERC), and Interactive Remote Access (IRA) "



Technical Rationale Lite

A High Level Summary of What changed and Why

Technical Rationale by Level of Change

Join: slido.com
#2016-02-D1a

- High Level of Change
  - CIP-005-7
  - CIP-010-5
- Moderate Level of Change
  - CIP-002-7
  - CIP-004-7
  - CIP-006-7
  - CIP-007-7
  - CIP-011-3
- Minor Level of Change
  - CIP-003-9
  - CIP-008-7
  - CIP-009-7
  - CIP-013-3

High Level of Change

Join: slido.com
#2016-02-D1a

CIP-005-7

- Logical isolation
  - ESPs with EAPs are a form of Logical Isolation, employing the perimeter model
  - Allows for the use of alternate models
    - Zero Trust Model
    - Hybrid Model
- Management Systems and Management Modules
  - Software Examples
    - VMware vCenter
    - Firewall Management Systems
  - Hardware Examples
    - Switch Management Interface
    - ILO Interface

High Level of Change

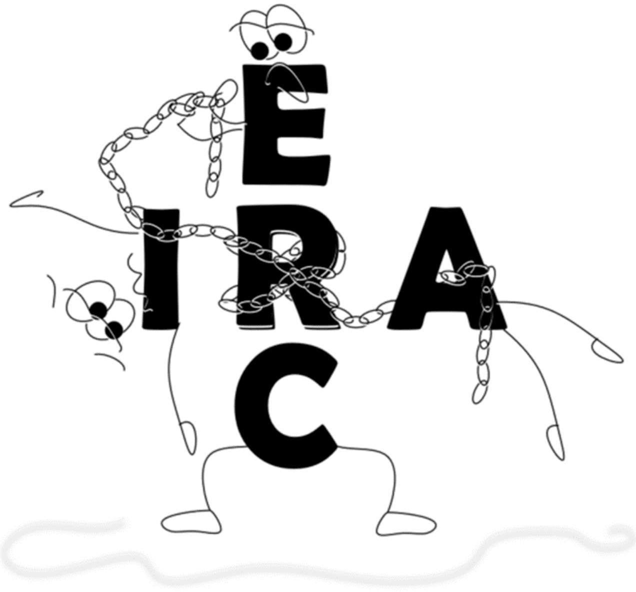
Join: slido.com #2016-02-D1a

CIP-005-7 (Continued)

- High Water Marking
  - Alternative to affinity for mixing BES Cyber Assets of differing impact ratings
    - Lower impact BES Cyber System assets become PCAs of higher impact BES Cyber System
    - Lower impact BES Cyber System assets are still BCAs of the lower impact BES Cyber System
- Super ESP
  - Single Network Segment which spans Physical Security Perimeters
  - Use Cases
    - Virtual Machine Migration
    - Software and Hardware Clustering Mechanisms
- CIP-006 R1.10
  - Replaced with CIP-005 R1.3

IRA and Changes CIP-005 Requirement R2

Join: slido.com
#2016-02-D1a



In response to the V5TAG request, the SDT proposes the following changes:

- Keep ERC with conforming changes in order to not disrupt its scoping function.
- Change the applicable systems scoping in CIP-005 Requirement R2 where needed from *Medium Impact BES Cyber Systems* ***with ERC*** to *Medium Impact BES Cyber Systems* ***with IRA***
- Simplify the IRA definition

IRA and Changes CIP-005 Requirement R2

Join: slido.com
#2016-02-D1a

The SDT proposes modifying the IRA definition so it becomes a simple glossary definition that:

- Removes embedded requirements and scoping mechanisms that were within it, and moves them to CIP-005 Requirement R2.
- References to ownership of the remote client become immaterial to the definition and CIP-005 requirements.
- “using a routable protocol” has been removed, thus no longer excluding serial protocol connections

Proposed Effect - IRA would include both serial and network connections for High and Medium Impact BCS.

Conforming Scoping Change in CIP-005 Requirement R2 and R3

Join: slido.com
#2016-02-D1a

The SDT proposes changing the applicable systems scoping in CIP-005-7 Requirement R2 Parts R2.4 and R2.5 :

- Add ***vendor remote access*** to *High Impact BES Cyber Systems*
- Change *Medium Impact BES Cyber Systems* ***with ERC*** to *Medium Impact BES Cyber Systems* ***with vendor remote access***

The SDT proposes the addition of Requirement R2 Part 2.6 - as it believes that affinity rules for Intermediate Systems running on Shared Cyber Infrastructure are appropriate

The SDT proposes only conforming changes to Requirement R3

High Level of Change

Join: slido.com
#2016-02-D1a

CIP-010-5

- Changes enable virtualization
- Added SCI to applicability
- Replaced the TFE concept with “per system capability”
- Remove reliance on “baseline”

High Level of Change

CIP-010-5

R1 Part 1.1

- Replaces CIP-010-4 R1 Parts 1.1-1.3
- Change Management vs. Baseline Configurations
    - Objective level requirement to authorize change
        - “Forward looking” to authorize changes
    - Adds SCI configuration items
    - Baselines become one tool an entity can use to track changes
- Parent/Child images
- Self-Contained Applications (SCA)
- SCI Configuration items

High Level of Change

Join: slido.com
#2016-02-D1a

CIP-010-5

Rest of R1

- Renumbered
- Removed “baseline”
- CEC Added to Parts 1.2.1 & 1.3.1
- Remediation VLANs

R2

- “unauthorized” changes

R3 Part 3.3

- Enabling remediation VLANs

Join: slido.com
#2016-02-D1a

Moderate Level of Change

CIP-002, CIP-004, CIP-006, CIP-007, and CIP-011

Moderate Level of Change

Join: slido.com
#2016-02-D1a

CIP-002-7

- CIP-002-6
  - Withdrawn at the NERC February 4, 2021 Board Meeting
  - Draft 2 will revert criterion 2.12 language to CIP-002-5.1a
  - Version moving forward will remain -7
- Share Cyber Infrastructure (SCI)
  - SCI is mutually exclusive of and roughly equivalent risk to BCS.
  - Add identification of SCI to R1
- Benefit
  - One requirement to place the mistake… instead of dozens

Moderate Level of Change

- CIP-004-7
  - Conforming changes to support virtualization
  - CIP Exceptional Circumstances - added to Requirement R3 Part 3.5
    - Cannot require PRA for certain situations such as first responders who require unescorted physical access.
  - IRA inclusion in applicability
    - To support V5TAG changes to IRA, The SDT proposes scoping the inclusion of IRA into applicability.
    - Medium Impact BCS without ERC were previously out of scope. These BCS could now fall into scope if IRA is present

Moderate Level of Change

Join: slido.com
#2016-02-D1a

CIP-006-7

- Applicability - scoping in each requirement has been crafted to include the SCI where appropriate - for virtualized PACS
- Existing non virtualized PACS - backwards compatibility exists
- Low impact and medium impact BCS with out ERC do not require PACS
- CEC moved to parent of R2 – Visitor Control Program (now includes Part 2.3 Visitor Logging) (note: missing strike out in Part 2.2)
- Consolidated CIP-006-7 R1 Part1.10 into CIP-005-7 R1 Part 1.3 to protect cabling that runs across the state and across the hall (aka Super ESP) . The proposed requirement was crafted so that backwards compatibility exists

Moderate Level of Change

Join: slido.com
#2016-02-D1a

CIP-007-7

- Main proposed changes are in Requirement R1
  - Part 1.1 now focuses on the network services that are available on a system rather the logical network ports that are being used - allowing for policy based controls
  - Part 1.3 (new) requires that only the needed network services be enabled on SCI and Management Modules of SCI
- Conforming changes other requirements

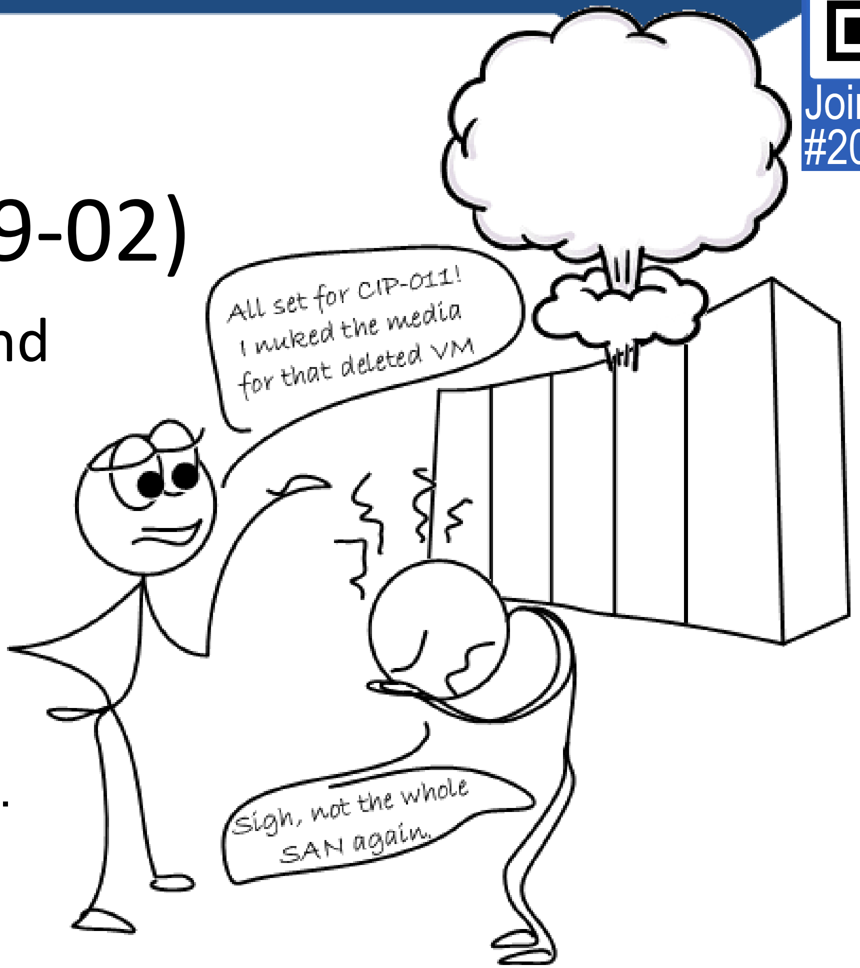
Moderate Level of Change

Join: slido.com #2016-02-D1a

CIP-011-3

Virtualization (2016-02) ≠ Cloud (2019-02)

- Changes apply to on-premise virtualized systems and environments only.
- R1 conforming changes to Applicable Systems
- R2 is an objective level requirement
  - Makes disposal and reuse a little more simple
  - Focus = protecting BES Cyber System Information (BCSI) rather than the physical ‘Cyber Assets’ and ‘storage media’.
  - Allows cryptographic erasure where BCSI cannot be mapped to particular disks within virtualized storage.


All set for CIP-011! I nuked the media for that deleted VM
Sigh, not the whole SAN again.

Method(s) to prevent the unauthorized retrieval of BCSI from applicable systems prior to their disposal or reuse (except for reuse within other systems identified in the “Applicable Systems” column)

Join: slido.com
#2016-02-D1a

Minor Level of Change

CIP-003-8, CIP-008-7, CIP-009-7, and CIP-013-3

Minor Level of Change

Join: slido.com
#2016-02-D1a

These are conforming changes to enable virtualization.

- CIP-003-8, CIP-008-7, CIP-009-7, CIP-013-3
  - Applicable Systems – Virtualized definitions matched to existing in scope BCS, EACMS, PCA, & PACS:
    - Updated for conformity with the new definitions including Shared Cyber infrastructure and Virtual Cyber Assets. These conforming changes to Applicable Systems make it clear the virtualized components are in scope, including SCI hosting BCS and associated EACMS, PCA, or PACS.

Implementation Plan

- 24 month implementation plan with provisions for early adoption.

- Early adoption – Entity and Regional Agreement to implement
  - Permits Registered Entities to work directly with their Region(s) to identify a date in advance of the 24 months to be compliant with the virtualization-enabled standards.
  - Responsible Entities must continue to comply with current enforceable CIP Standards and Definitions until that agreed upon Early Adoption date.

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Final Survey

Part 2

Upcoming webinar

March 3, 2021

2:00 – 4:00 p.m. Eastern

Submit topics in slido survey

Join at

slido.com

#2016-02-D1a

RELIABILITY | RESILIENCE | SECURITY

Resources

Join: slido.com
#2016-02-D1a

- This slide deck and other information relative to the CIP Modifications SDT may be found on the Project 2016-02 Project Page under Related Files:

  http://www.nerc.com/pa/Stand/Pages/Project%202016-02%20Modifications%20to%20CIP%20Standards.aspx

- The Informational Filing of the North American Electric Reliability Corporation Regarding Standards Development Projects latest filing can be found here:

  https://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/CIP%20SDT%20Schedule%20 %20Dec_2020_Informational%20Filing.pdf

- Project 2016-02 Related Files Pages for previous webinar recordings: https://www.nerc.com/pa/Stand/Pages/Project-2016-02-Modifications-to-CIP-Standards-RF.aspx

Resources Continued

Join: slido.com
#2016-02-D1a

- Project 2016-02 Related Files Pages for previous webinar recordings:

  https://www.nerc.com/pa/Stand/Pages/Project-2016-02-Modifications-to-CIP-Standards-RF.aspx

- Specific Recommended Webinars:
  - Management Systems (LINK)
  - SuperESP (LINK)
  - Virtual Machines and Containers (LINK)
  - Hypervisor and Storage Systems (LINK)
  - External Routable Connectivity and Interactive Remote Access (LINK)
  - CIP-005 and Zero Trust (LINK)

Join: slido.com
#2016-02-D1a

Questions and Answers

Final Remarks

Join: slido.com
#2016-02-D1a

- Help us prepare for the March 3rd webinar.
  - Send topic recommendations by 5:00 PM Thurs Feb 25, 2021
  - Submissions can be emailed to jordan.Mallory@nerc.net