DRAGOS

SANS

NERC CIP RELIABILITY STANDARDS

CONTINUOUS IMPLEMENTATION PROJECT
OR CHANGE INDUCED PANIC?

PRINCIPAL CYBER RISK ADVISOR
SANS INSTRUCTOR

ICS CURRICULUM DIRECTOR
SANS INSTRUCTOR

NERC CIP RELIABILITY STANDARDS

CONTINUOUS IMPLEMENTATION PROJECT OR CHANGE INDUCED PANIC?

BUILT BY PRACTITIONERS FOR PRACTITIONERS

600+ YEARS OF ICS/OT EXPERIENCE

210+ EMPLOYEES

150+ CUSTOMERS

20 COUNTRIES

10 INDUSTRY VERTICALS

Dragos has the largest team of ICS security specialists in the industry which allows us to make the best technology.

- ELECTRIC
- OIL & GAS
- MANUFACTURING
- BLDG AUTO SYS
- CHEMICAL
- WATER
- FOOD & BEV
- MINING
- TRANSPORTATION
- PHARMACEUTICAL

Including **9** of the **10** largest U.S. electric utilities and **5** of the **10** largest oil and gas companies

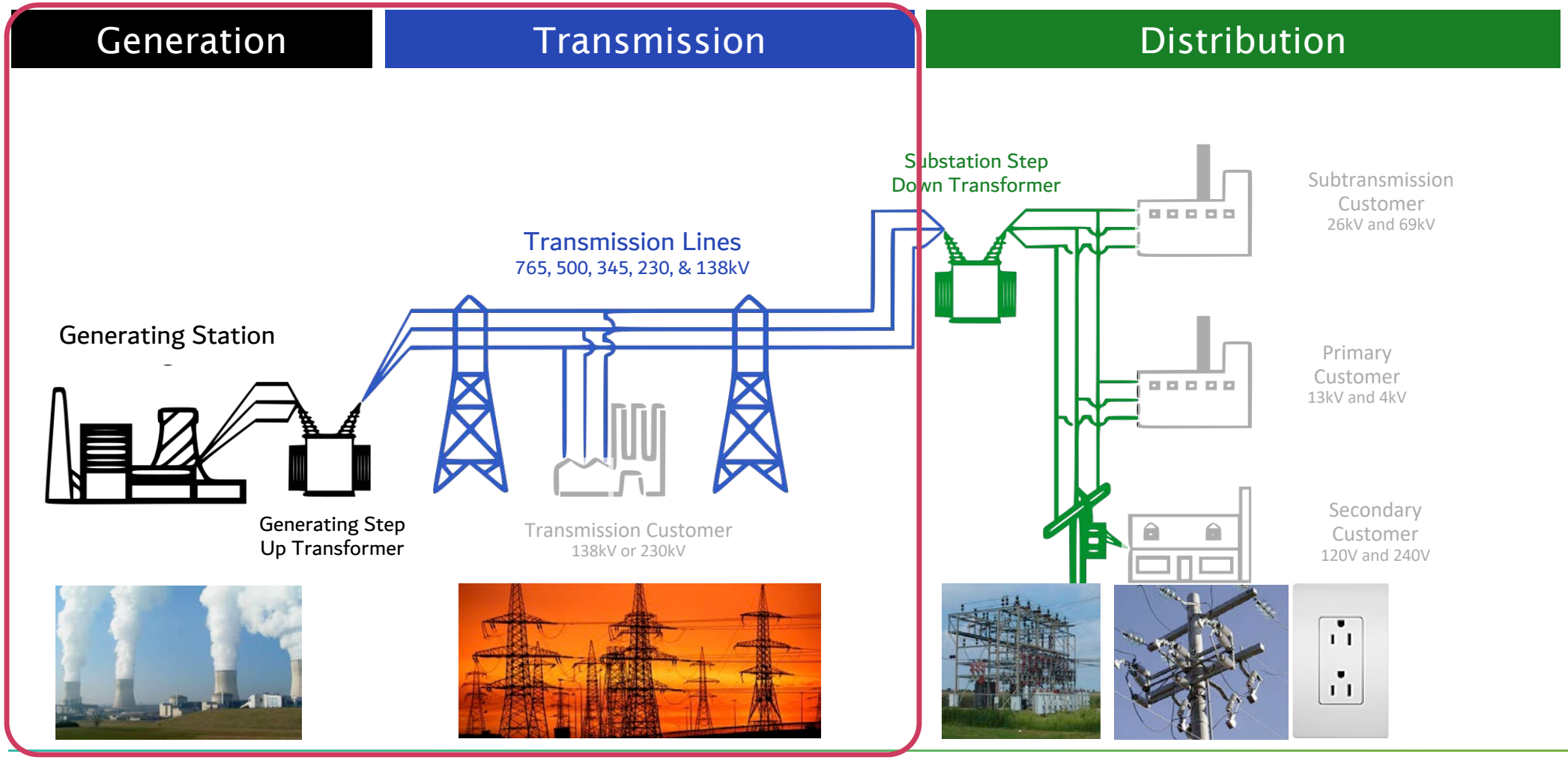
HQ | Hanover, MD

REGIONAL | Canada, Australia, GCC, UK/Europe

ELECTRIC SECTOR
&
NERC CIP

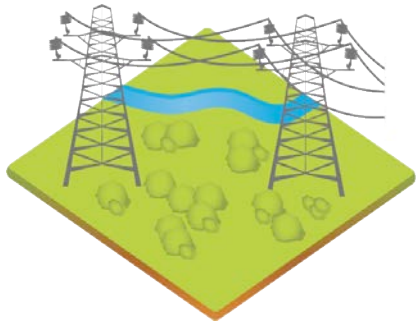
THE ELECTRIC SECTOR

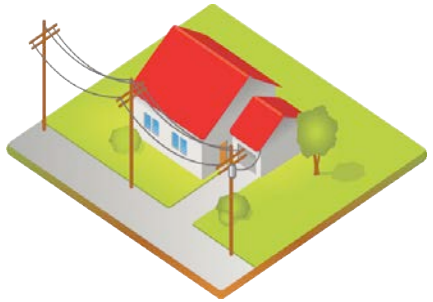
AN INTRODUCTION



THE ELECTRIC SECTOR

AN INTRODUCTION

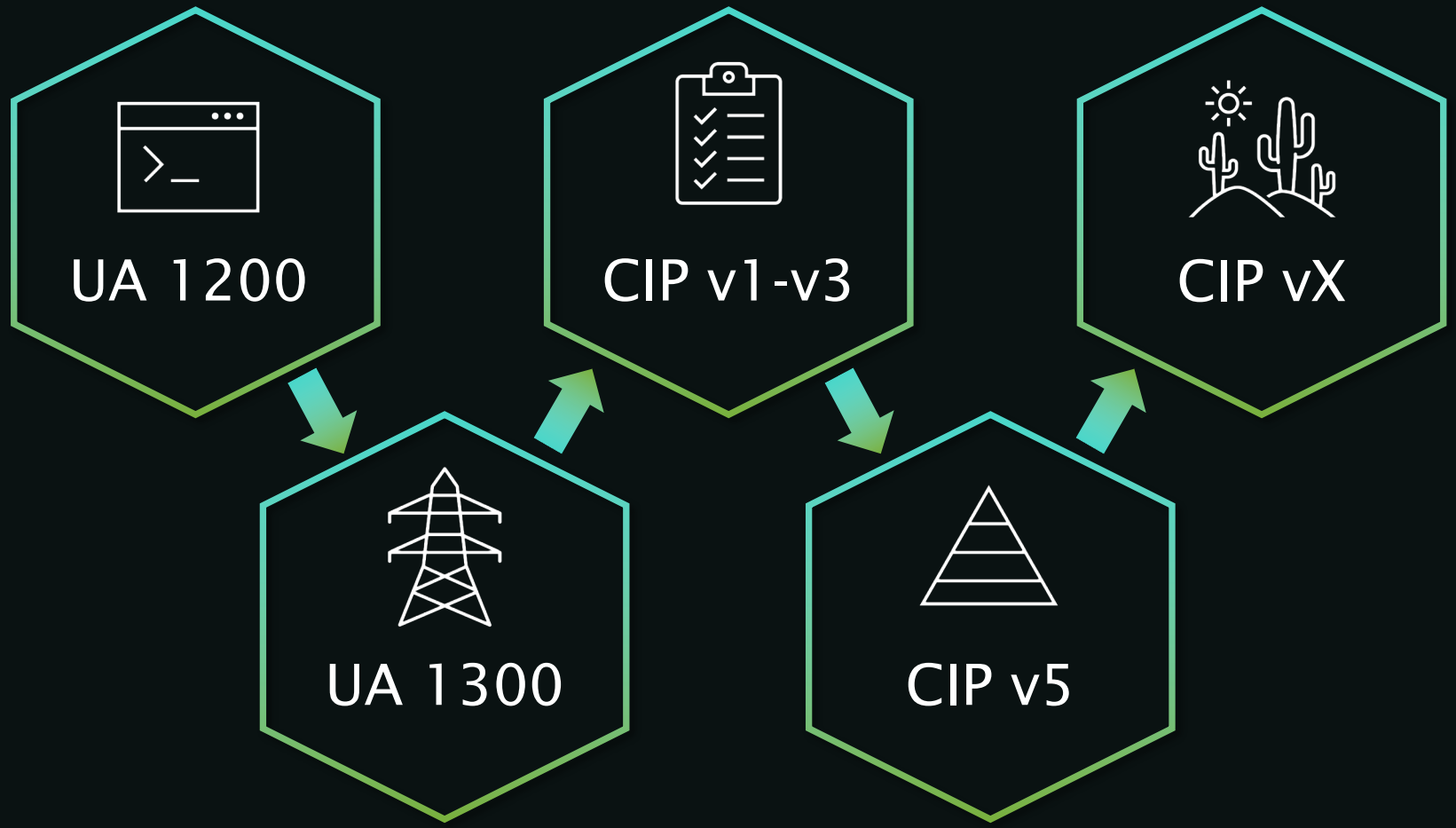




Generation	Transmission	Distribution
5,000 plants	160,000 miles	Over 1,000,000 miles
65% of monthly bill	5% of average customer monthly bill	30% of average customer monthly bill
Employs approx. 120,000 people nationwide	Employs approx. 15,000 people nationwide	Employs approx. 400,000 people nationwide

THE CIP JOURNEY

HOW WE GOT HERE



Current NERC CIP Standards

Number & Version	Standard Name
CIP-002-5.1	BES Cyber System Categorization
CIP-003-8	Security Management Controls
CIP-004-6	Personnel & Training
CIP-005-6	Electronic Security Perimeter(s)
CIP-006-6	Physical Security of BES Cyber Systems
CIP-007-6	System Security Management
CIP-008-5	Incident Reporting & Response Planning
CIP-009-6	Recovery Plans for BES Cyber Systems
CIP-010-3	Configuration Change Management & Vulnerability Assessments
CIP-011-2	Information Protection
CIP-012-1	Communications Between Control Centers
CIP-013-1	Supply Chain Risk Management
CIP-014-2	Physical Security

UTILITY PERSPECTIVES

CHALLENGES IN CIP COMPLIANCE

- “Zero deficiency” requirements
- Regional differences in audits and techniques
- Lack of clarity on “how to comply” *(double-edged sword)*
- Evidence collection is burdensome
- Process, people, and technology limits
- “Compliance does not equal security”

REGULATORY PERSPECTIVES

CHALLENGES IN CIP ENFORCEMENT

- “Is enough covered?”
- Lack of evidence could mean lack of security
- Compliance needs to be “baked in” to security
- Process, people, and technology limitations

THE NUANCED TRUTH

OBSERVATIONS FROM THE FRONT LINES

"The root causes of these violations were cultural issues that resulted in URE management's lack of awareness, engagement, and accountability for CIP compliance."

VIOLATIONS ARE INCREASING

Since CIPv5, there has been an uptick in possible violations across industry.

INDUSTRY IS IMPROVING

Lessons learned are being applied, industry exercises are mature national-level events.

MIXED CULTURAL IMPACTS

With ~2000 utilities that must comply, some "get it," others do not.

AWESOME.
SO WHAT NOW?

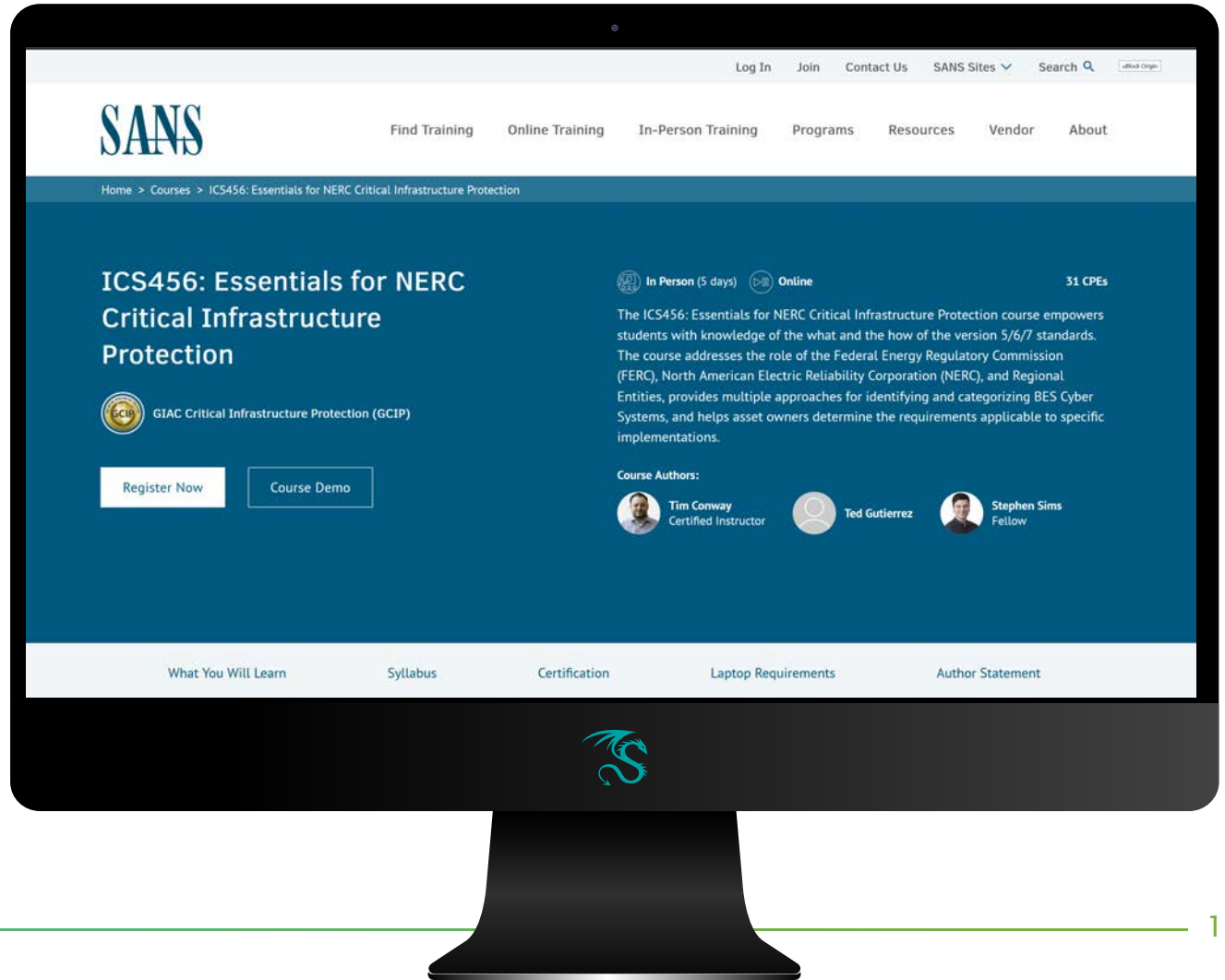
Agenda


Incident Response
Supply Chain
Virtualization
Control Center Comms
Executive Orders

PRACTICAL GUIDANCE FROM PRACTITIONERS

LEVERAGING ICS456 FOR NERC CIP ESSENTIALS

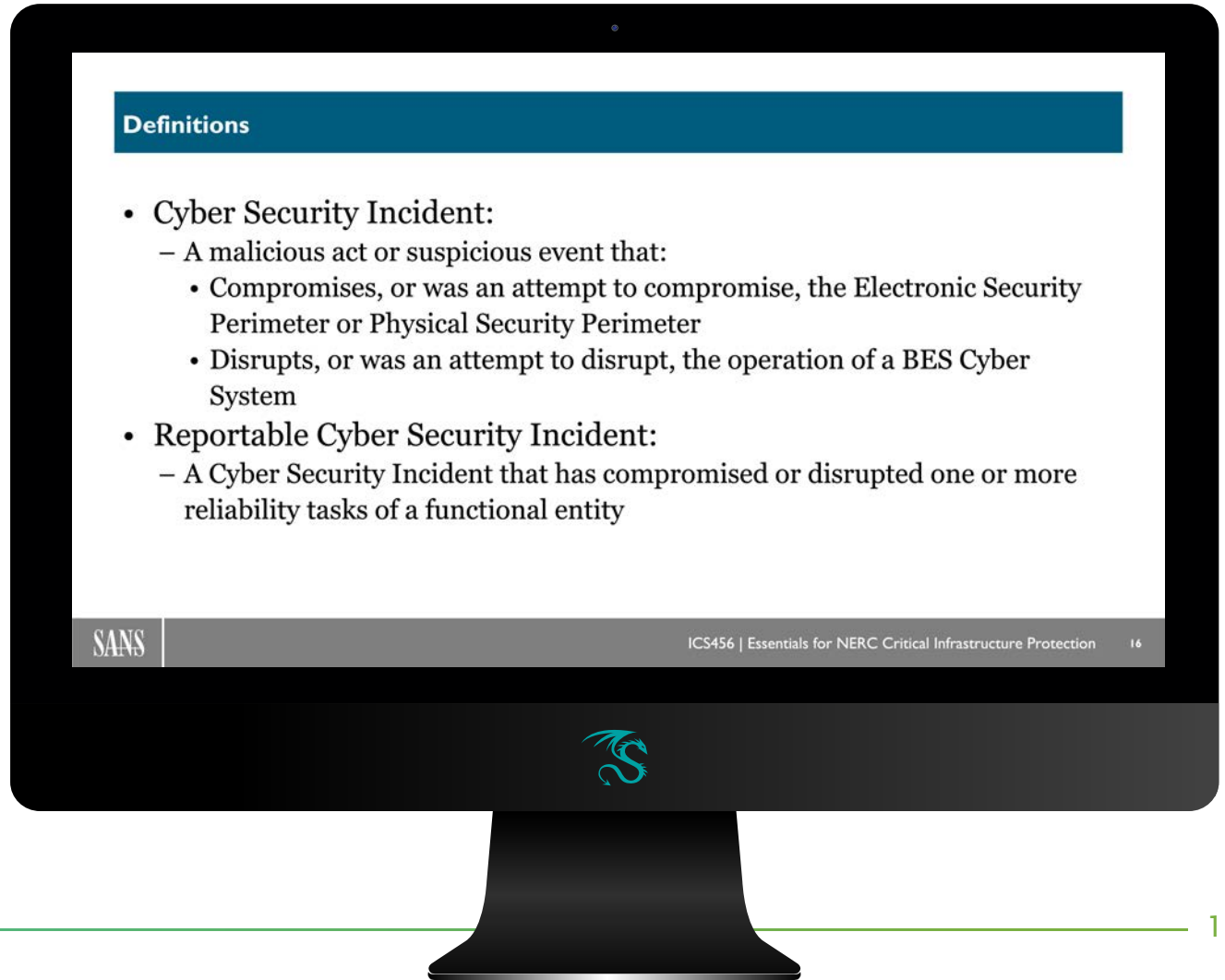
- Over 3 years and hundreds of students
- Demonstrate foundational knowledge with the GCIP certification
- “Not just compliance” with over 20 hands-on labs
- Links regulation with technical capabilities
- Now OnDemand!



PRACTICAL GUIDANCE FROM PRACTITIONERS

LEVERAGING ICS456 FOR NERC CIP ESSENTIALS

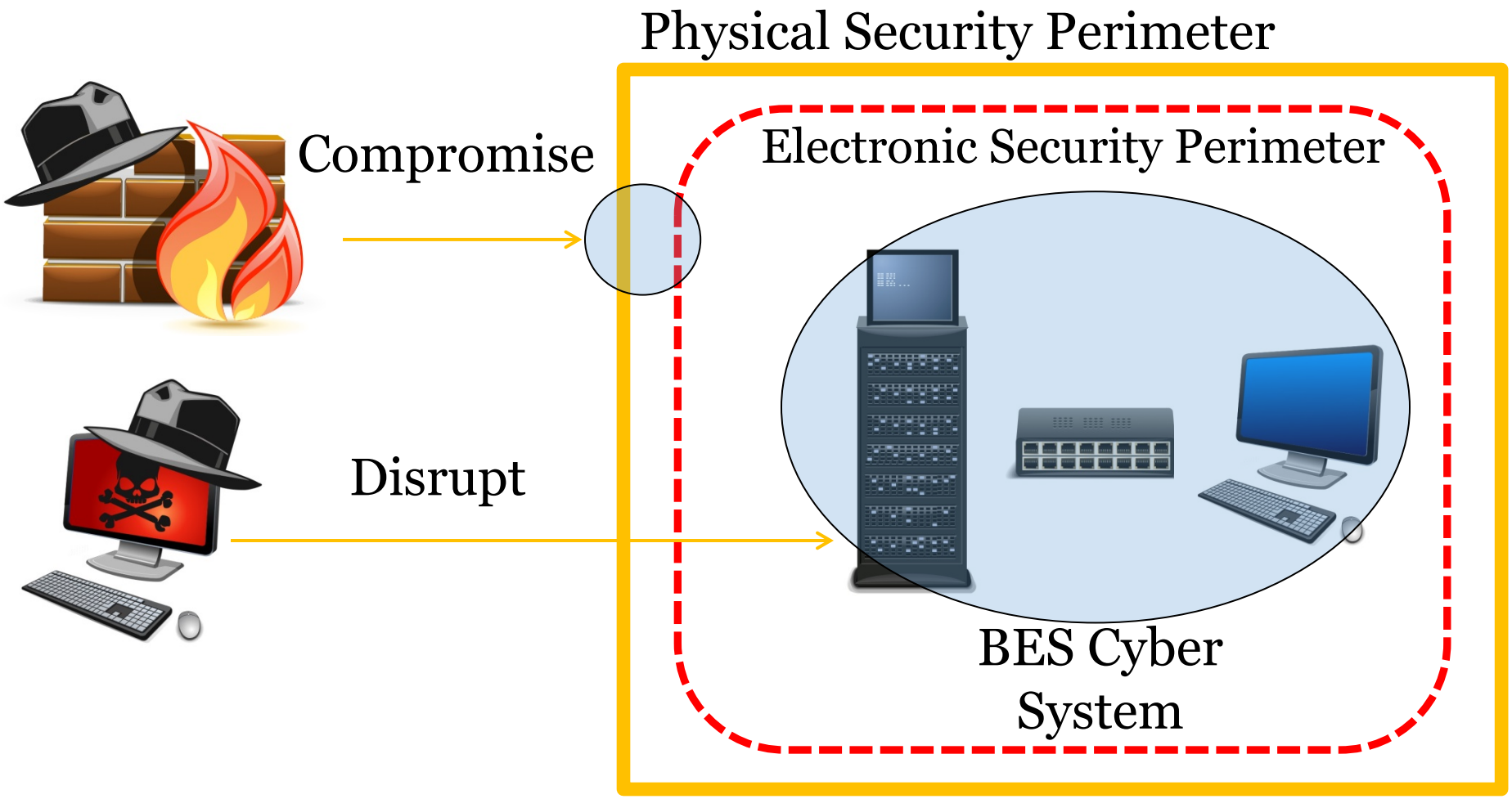
- Sneak peek at content and some key “boots on the ground” takeaways.
- Usually updated when standards are mandatory…
  - But when has 2020 been “business as usual?”
- Let’s launch into some class time!



Definitions

- Cyber Security Incident:
  - A malicious act or suspicious event that:
    - Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter
    - Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System
- Reportable Cyber Security Incident:
  - A Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity

Soon to be History



Change Is Very Near - Jan 1, 2021

164 FERC ¶ 61,033
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

18 CFR Part 40

[Docket No. RM18-2-000; Order No. 848]

Cyber Security Incident Reporting Reliability Standards

(Issued July 19, 2018)

AGENCY: Federal Energy Regulatory Commission.

ACTION: Final rule.

SUMMARY: The Federal Energy Regulatory Commission (Commission) directs the North American Electric Reliability Corporation (NERC) to develop and submit modifications to the NERC Reliability Standards to augment the mandatory reporting of Cyber Security Incidents, including incidents that might facilitate subsequent efforts to harm the reliable operation of the bulk electric system (BES).

- Report—compromise, or attempt to compromise, the ESP or associated EACMS
- Require minimum reporting detail
- Reporting timeline
- Reporting to DHS as well as E-ISAC
- NERC to develop summary reports to FERC

CIP-008 R4 – Notifications and Reporting for Cyber Security Incidents

- Notify E-ISAC and NCCIC of Reportable CSI and <u>attempts</u> to compromise: [6]
  - Initial notification and updates to include:
    - Functional impact
    - Attack vector used; and
    - Level of instruction achieved or attempted
  - Initial notification:
    - within 1-hour of determination of **<u>Reportable CSI,</u>**
    - end of next calendar day after attempt to compromise
  - Update E-ISAC and NCCIC within 7-days of learning new attribute information

National Cybersecurity and Communications Integration Center - NCCIC

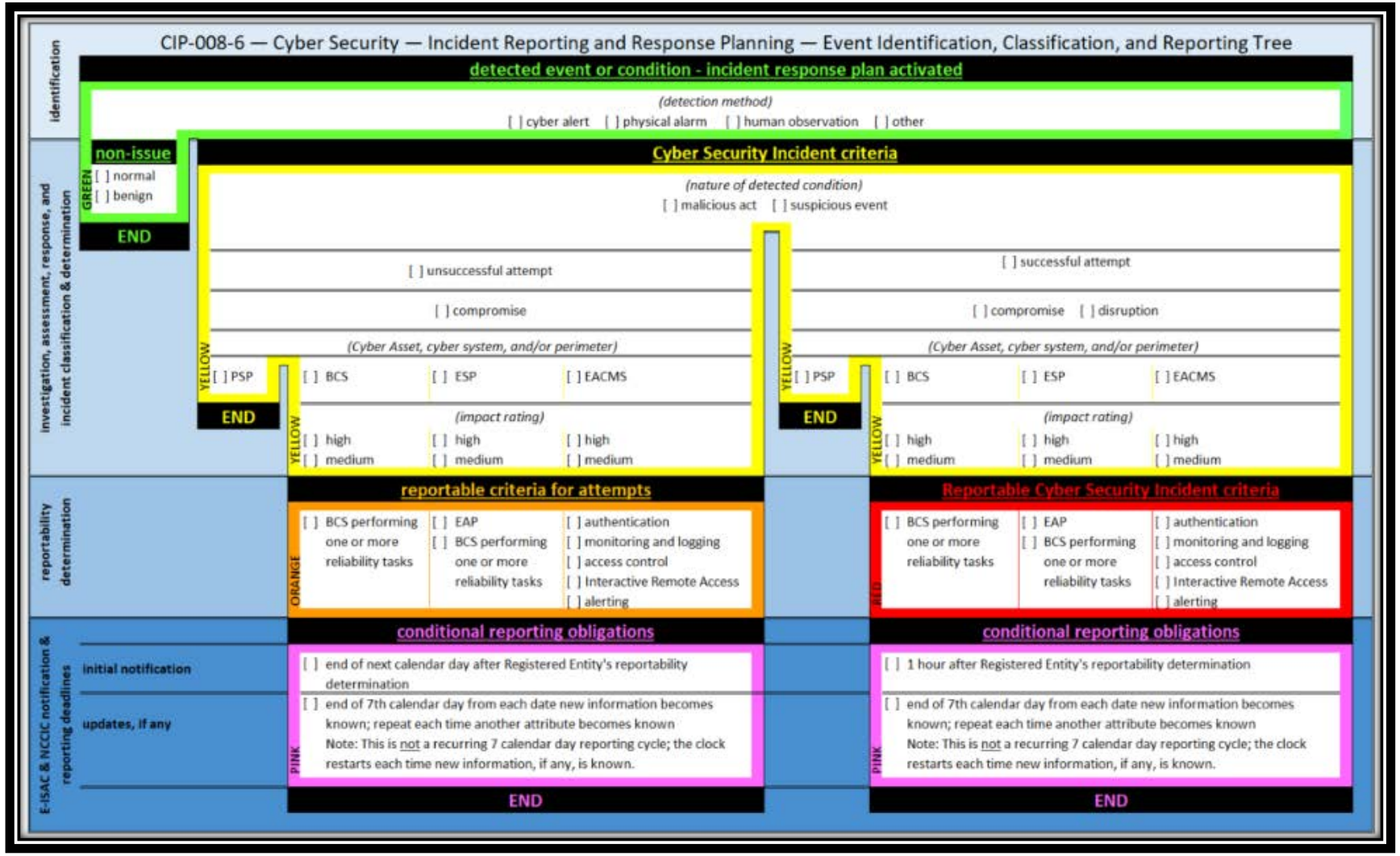
The NCCIC has a history stemming from many legacy organizations and is comprised of four main branches today:

- NCCIC Operations & Integration (NO&I);
- United States Computer Emergency Readiness Team (US-CERT);
- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT); and
- National Coordinating Center for Communications (NCC).

Significant Effort to Provide Guidance

Cyber Security – Incident Reporting and Response Planning

Implementation Guidance for CIP-008-6



CIP-008-6 Incident Reporting and Response Planning (2018-02 SDT)

- Implementation guidance has been submitted for ERO endorsement
- November 5th ERO decided not to endorse the CIP-008 implementation guidance which included specific guidance on how to categorize assessments and reporting detail

The ERO Enterprise declined to endorse this proposed Implementation Guidance document because there are several concerns within the document which resulted in the guide not receiving an unanimous vote to endorse. To summarize the concerns, the guide is clearer than the previous version submitted; however, some statements are not appropriate for Implementation Guidance. These statements may be viewed as an ERO Enterprise audit approach and / or directing CMEP staff decision making. Inconclusion, the ERO Enterprise is not planning on endorsing the guidance; however, we will be providing detailed feedback to the drafters

Agenda


Incident Response
Supply Chain
Virtualization
Control Center Comms
Executive Orders

CIP-012 R1 Securing Real-time Comms between Control Centers – eff. 7/1/2022

- Implement documented plan(s) to mitigate the risks of disclosure and modification of Real-time Assessment and Real-time monitoring data while in transit between Control Centers:
  - Except under CIP Exceptional Circumstances…
  - Identify security protection used to mitigate the risks [1]
  - Identify applied security protection for transmitting Real-time Assessment and Real-time monitoring data between Control Centers; and
  - If owned or operated by different Responsible Entities, identification of responsibilities

Communicating between Control Centers

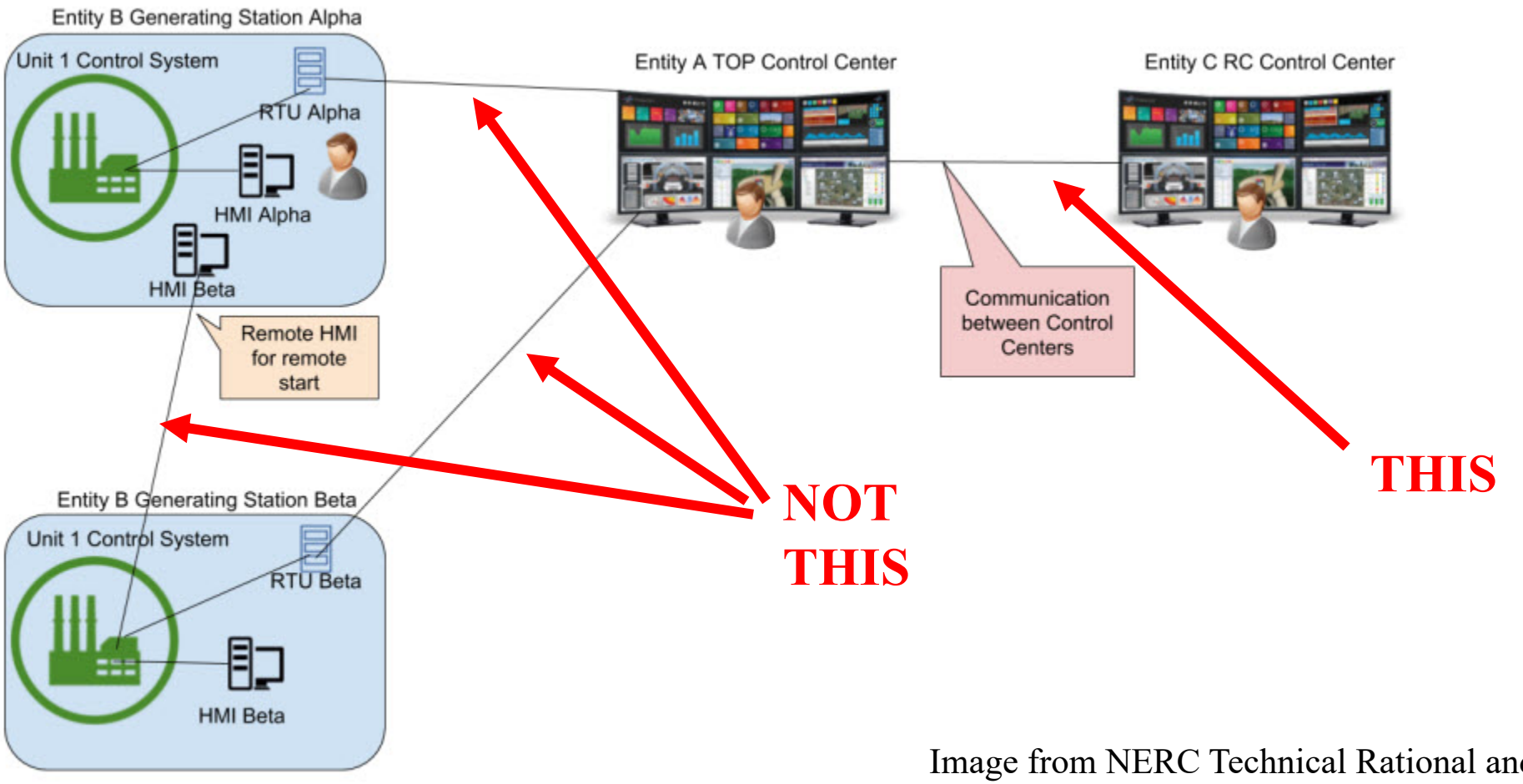
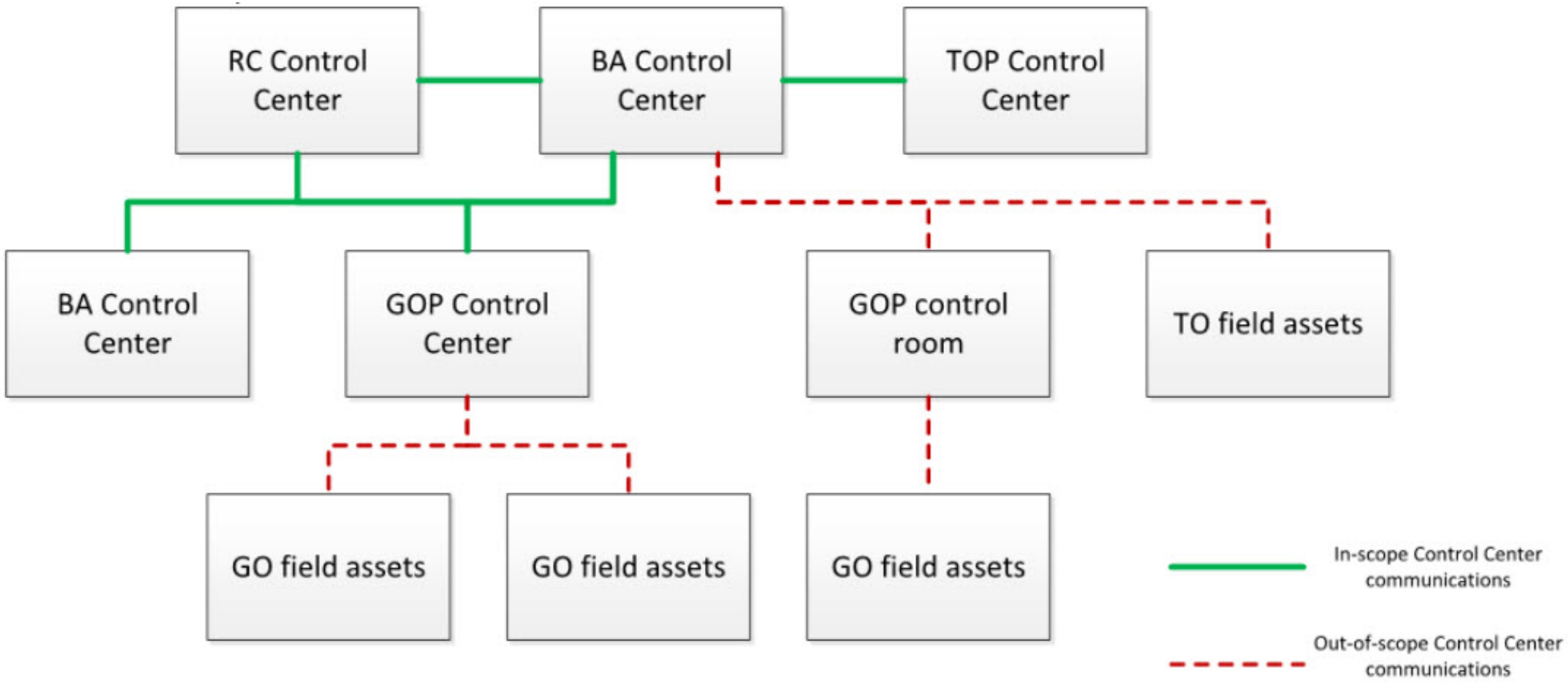
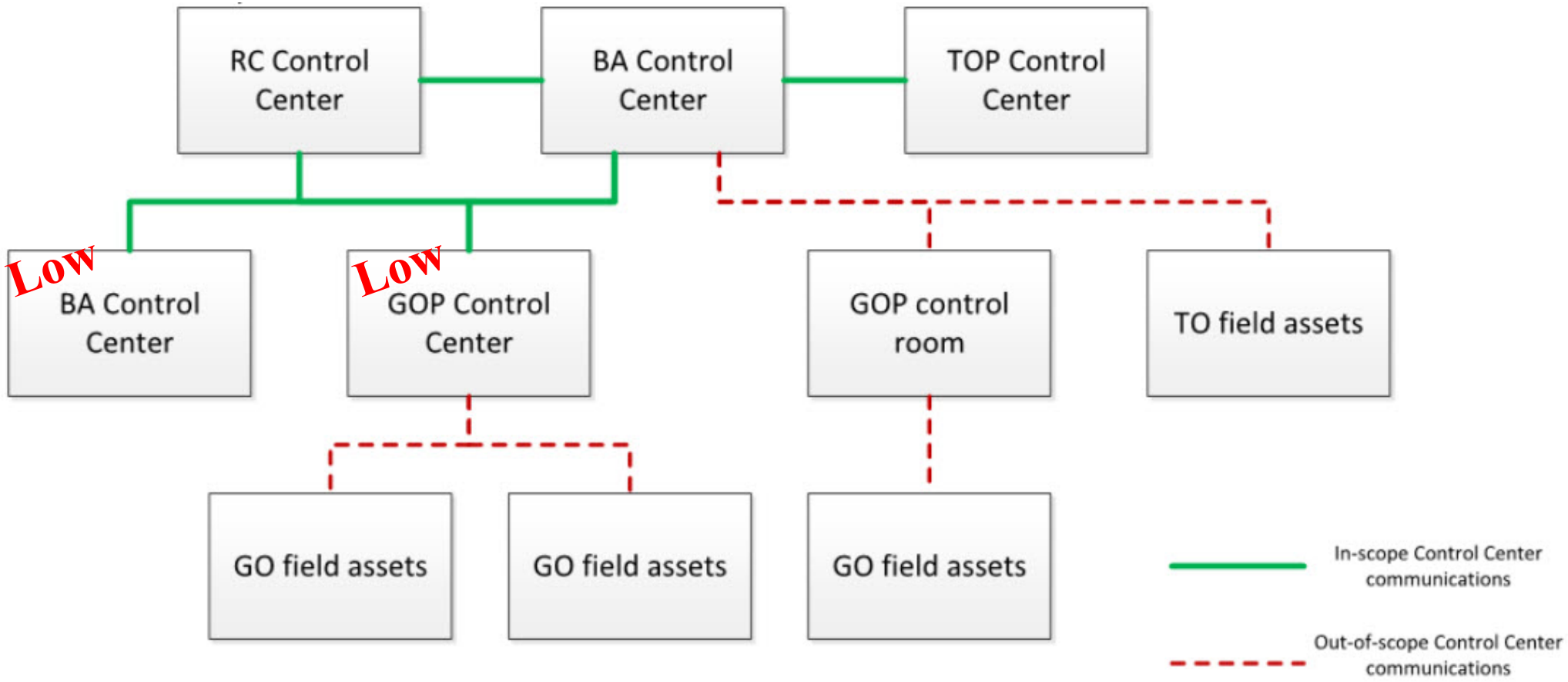


Image from NERC Technical Rational and Justification for CIP-012-1

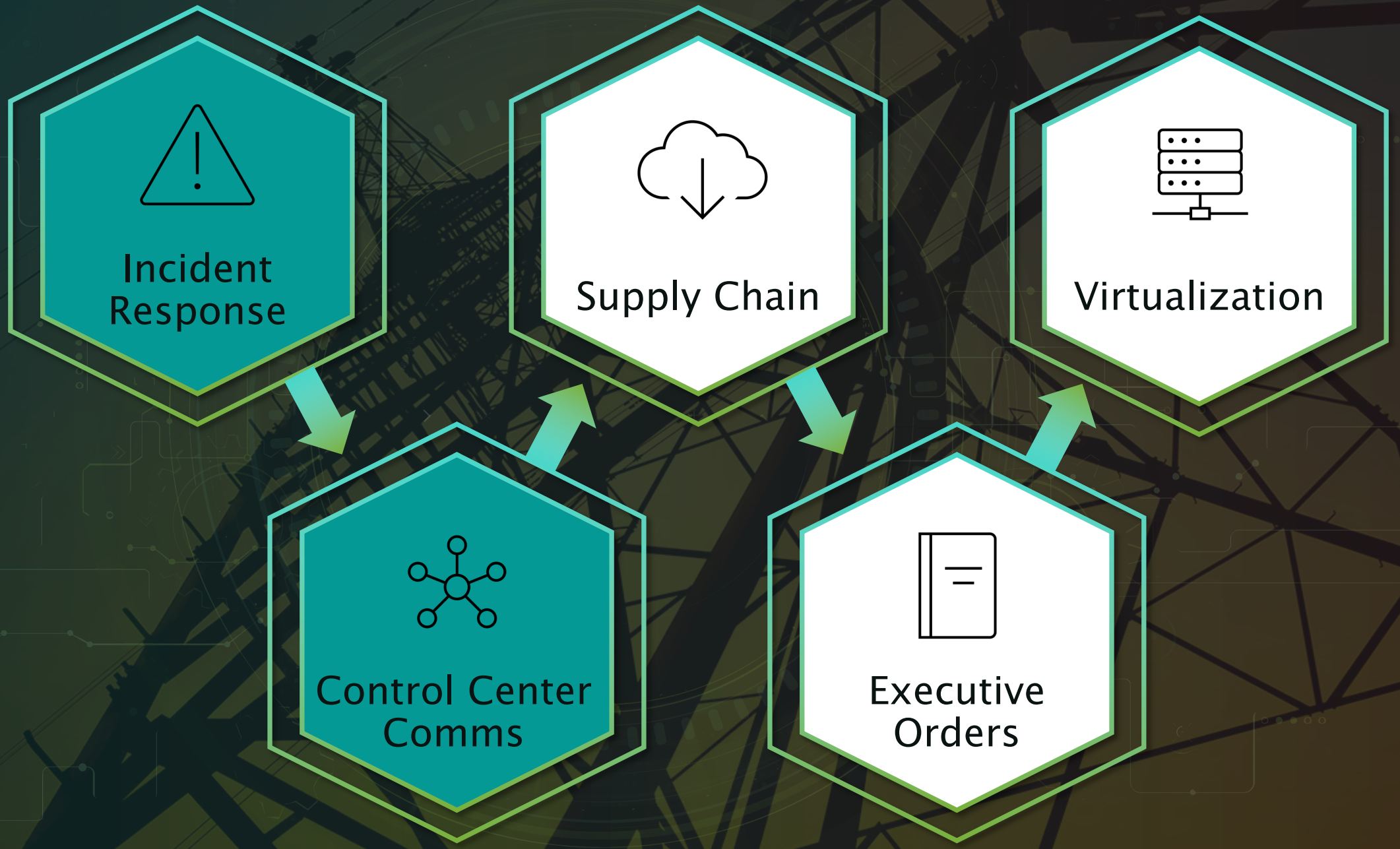
Reference Model: Control Centers In Scope



Reference Model: Control Centers In Scope



Agenda


Incident Response
Supply Chain
Virtualization
Control Center Comms
Executive Orders

CIP-013 R1 Supply Chain Risk Management (SCRM) Plan(s) – eff 10/1/2020

- Develop documented supply chain cyber security risk management plan(s): [1]
  - Process used in planning for procurement of BES Cyber Systems (hardware and software) to identify risk(s) to the BES including the transitioning from one vendor to another.
  - Process used to procure BES Cyber Systems that address:
    - Notification by the vendor to the RE of incidents that pose cyber security risks to the RE
    - Coordination of responses with the vendor
    - Notification by the vendor when remote or on-site access should no longer be granted to vendor representatives
    - Disclosure by vendors of known vulnerabilities
    - Verification of software integrity and authenticity of all software and patches provided by the vendor
    - Coordination of controls for (i) vendor-initiated Interactive Remote Access, and (ii) system-to-system remote access with a vendor(s).

CIP-013 R1 Documented Processes and Procurement Plan

R1.1 - Acknowledge there is a Concern in Procurement

- Identify and document cyber security risks related to:
  - Installing vendor equipment and software
  - Transitioning from one vendor to another

R1.2 - Future Procurement Contracts Need to Address

- Vendor notification of vendor incidents
- Coordination of response to vendor incidents
- Notification of remote or onsite access revocation
- Vendor Vulnerability disclosure
- Verification of software integrity and authenticity
- Coordination of controls for vendor IRA and system-to-system remote access

Help With R1.1 – NIST Supply Chain Risk Management Guidance

- NIST Special Publication 800-161
- Risk Management approach examining;
  - Supply Chain Threats;
  - Supply Chain Vulnerabilities;
  - The likelihood of a threat exploiting a vulnerability;
  - And the impact of that event
- Focus on Federal Agency Information and Communications Technology (ICT) Supply Chain Risk Management

NIST SP 800-161 ICT Supply Chain Risk Model

ICT Supply Chain Risk

Threats	Vulnerabilities
Adversarial: e.g., insertion of counterfeits, tampering, theft, and insertion of malicious software.	External: e.g., weaknesses to the supply chain, weaknesses within entities in the supply chain, dependencies (power, telecom, etc.)
Non-adversarial: e.g., natural disaster, poor quality products/services and poor practices (engineering, manufacturing, acquisition, management, etc.).	Internal: e.g., information systems and components, organizational policy/processes (governance, procedures, etc.)

Likelihood (probability of a threat exploiting a vulnerability(s))

Adversarial: capability and intent	Non-adversarial: occurrence based on statistics/history

Impact - degree of harm

To: mission/business function	From: data loss, modification or exfiltration
	From: unanticipated failures or loss of system availability
	From: reduced availability of components

Risk

Help With R1.2 – EEI Model Procurement Contract Language

EEI
Edison Electric
INSTITUTE

Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk

Version 1.0

Requirement R1.2.2

Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity.

EEI Model Procurement Contract Language

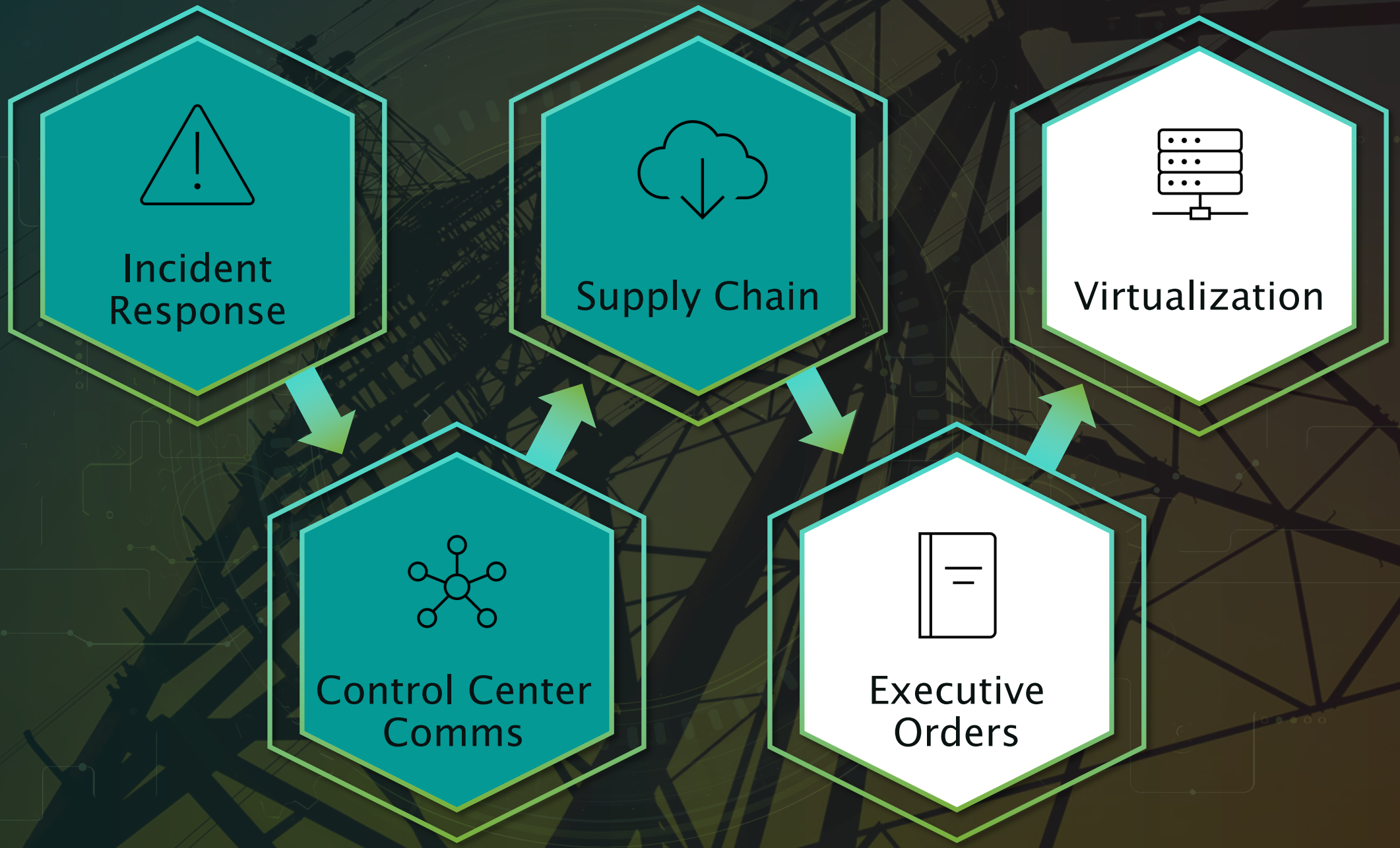
Development and Implementation of a Response Plan: Contractor shall develop and implement policies and procedures to address Security Incidents ("Response Plan") by mitigating the harmful effects of Security Incidents and addressing and remedying the occurrence to prevent the recurrence of Security Incidents in the future.[5] Contractor shall provide Company access to inspect its Response Plan. The development and implementation of the Response Plan shall follow best practices that at a minimum are consistent with the contingency planning requirements of NIST Special Publication 800-61 Rev. 2[6], NIST Special Publication 800-53 Rev. 4, CP-1 through CP-13[7] and the incident response requirements of NIST Special Publication 800-53 Rev. 4, IR-1 through IR-10 as those standards may be amended.[8]

Immediately upon learning of a Security Incident related to the products and services provided to Company, Contractor shall implement its Response Plan and, within 24 hours of implementing its Response Plan, shall notify Company of that implementation by contacting [insert contact name].

CIP-013 R2 and R3 Implement and Review

- R2 - Implement supply chain cyber security risk management plan(s) [1]
  - Does not require renegotiation of existing contracts nor does the requirement apply to the Terms and Conditions of contracting language
  - Demonstrate "implementation" with vendor correspondence documents, policy documents, or working documents that reflect the use of the SCRM plan developed for R1
- R3 - CIP Senior Manager or delegate plan review and approval every 15 calendar months
  - Approved plan(s)
  - Evidence of review of the plan(s)

Agenda


Incident Response
Supply Chain
Virtualization
Control Center Comms
Executive Orders

RECENT ACTIVITIES

RESPONDING TO THE WHITE HOUSE ACROSS DOE & FERC

It's been a busy year of activity for grid security– without exaggeration, there has been more focus from lawmakers in 2020 than there has been in almost a decade.

Here's what utilities need to know:

SUPPLY CHAIN EXECUTIVE ORDER

- Require(d?) wide-reaching discussions with utilities
- Some lightening rod topics in DOE's Request for Information
- Follow-up order from FERC issued

FERC RATE INCENTIVES

- Links traditional regulatory affair considerations with security professionals
- ROE devices for security investments

NERC CIP IMPROVEMENT

- FERC is seeking input on ways to improve NERC CIP, with an increased focused on Low Impact facilities
- Leverages NIST CSF

THE DISCUSSIONS WE HAD

…THE JOYS OF REGULATORY COMMENT PERIODS…

Via Electronic Filing
Deputy Assistant Secretary Charles Kosak
Office of Electricity, Transmission Permitting and Technical Assistance Division
Department of Energy
1000 Independence Avenue SW
Washington, DC 20585

Dear Mr. Kosak,

Pursuant to the issuance of Executive Order 13920 (85 FR 26595) and the US Department of Energy's request for information (85 FR 41023), please find the selected responses and recommendations of Messrs. Jason Christopher, Tim Conway, and Patrick Miller.

The respondents have individually worked within the electric sector over the past two decades and collectively bring a variety of different perspectives in roles held at: large vertically integrated utilities in an asset owner-operator role, within government roles at the Federal Energy Regulatory Commission ("FERC" or "the Commission"), within the Department of Energy ("DOE" or "the Department"), as DOE contractors within the national labs, consultants to power utilities, consultants to control system vendors, and as North American Electric Reliability Corporation ("NERC") regional auditors. The respondents appreciate the open and transparent nature of the Request for Information ("RFI") issued by DOE and believe this is an important opportunity to provide feedback from the various perspectives held by the respondents throughout their careers. The respondents have identified general themes in their response, including the need for:

- Improving alignment between EO 13920's four main pillars and the RFI questions pertaining to supply chain; organization risk assessments, organization FOCI consideration practices, vulnerability management programs, ICS protocol security, and information sharing. The respondents all strongly agree that each of these items identified in the RFI questions are relevant items for entities to focus on and address in their security programs; however, the questions referenced within these items appear to have the potential to expand the scope of the Executive Order. Some of the questions reference concepts not introduced in the Executive Order.
- Building any additional supply chain capabilities needs to align with current BPS regulations, regulatory efforts underway to modify current standards, and should consider industry activities to implement these requirements. Changes or modifications to current approaches in effect, or going into effect, could add delays to the implementation of the new supply chain regulations, including any continuous improvement efforts.
- Additional context, FAQ documentation, or reference guides to establish intent of questions in relation to the Executive Order scope. There is risk of entity reluctance to respond due to the various interpretations available for each of the questions, which will result in difficulty for DOE to draw appropriate conclusions based on responses received.

Thank you for your consideration in this matter,

Sincerely,

Jason D. Christopher Tim Conway Patrick Miller

August 24, 2020
Via Electronic Filing
Ms. Kimberly D. Bose
Federal Energy Regulatory Commission
888 First Street NE
Washington, DC 20426

Dear Ms. Bose,

Pursuant to the Notice of Inquiry on Potential Enhancements to the Critical Infrastructure Protection Reliability Standards (Docket No. RM20-12-000), please find the selected responses and recommendations of Messrs. Jason Christopher and Tim Conway.

The respondents have individually worked within the electric sector over the past two decades and collectively bring a variety of different perspectives in roles held at: large vertically integrated utilities in an asset owner-operator role, within government roles at the Federal Energy Regulatory Commission ("FERC" or "the Commission"), within the Department of Energy ("DOE" or "the Department"), as DOE contractors within the national labs, consultants to power utilities, and as consultants to control system vendors. The respondents appreciate the open and transparent nature of the Notice of Inquiry ("the Notice") issued by the Commission and believe this is an important opportunity to provide feedback from the various perspectives held by the respondents throughout their careers. The respondents have identified general themes in their response:

- **On Enhancing the CIP Reliability Standards:** Based on the questions in the Commission's Notice, the respondents note that the particular controls under examination already exist in the CIP Reliability Standards, including the policies for Low Impact BES Cyber Systems. While evaluating discussions about information availability, as an example, the entirety of Reliability Standards should be considered, such as those dedicated for Real-time Assessments and operations.
- **Regarding coordinated cyber attacks:** There are many existing requirements which can help utilities manage new threats. The respondents note that several industry efforts are not mandatory under the CIP Reliability Standards, but could be covered under an existing CIP program. Where possible, the Commission could provide industry-based guidance or other voluntary measures to encourage adoption, such as those highlighted in the recent Notice of Cybersecurity Incentives White Paper.

The attached responses also provide additional context and comparison of the proposed incentives, including a nuanced discussion of the CIP Reliability Standards and the National Institute of Standards and Technology ("NIST") Cybersecurity Framework. As Commission staff knows, these two different collections of controls and requirements were created to serve different purposes and, as such, their uses will be varied across the electric sector.

Thank you for your consideration in this matter,

Sincerely,

Jason D. Christopher Tim Conway

August 24, 2020
Via Electronic Filing
Ms. Kimberly D. Bose
Federal Energy Regulatory Commission
888 First Street NE
Washington, DC 20426

Dear Ms. Bose,

Pursuant to the public release of the Cybersecurity Incentives Policy White Paper (Docket No. AD20-19-000), please find the selected responses and recommendations of Messrs. Jason Christopher, Tim Conway, and Patrick Miller.

The respondents have individually worked within the electric sector over the past two decades and collectively bring a variety of different perspectives in roles held at: large vertically integrated utilities in an asset owner-operator role, within government roles at the Federal Energy Regulatory Commission ("FERC" or "the Commission"), within the Department of Energy ("DOE" or "the Department"), as DOE contractors within the national labs, consultants to power utilities, consultants to control system vendors, and as North American Electric Reliability Corporation ("NERC") Critical Infrastructure Protection ("CIP") regional auditors. The respondents appreciate the open and transparent nature of the Notice of White Paper ("the Notice") issued by the Commission and believe this is an important opportunity to provide feedback from the various perspectives held by the respondents throughout their careers. The respondents have identified general themes in their response, including the need for:

- **Clarity regarding expanding the scope of NERC CIP requirements for incentivization**. Many utilities may find advantages to taking used and useful technologies used for NERC CIP compliance. Depending on the technology, there may be cost-effective and scalable options for expanding coverage to currently out-of-scope assets and facilities. However, non-CIP data and assets may now be reviewed in Federal Power Act Section 215 audits as a result, causing potential issues with regional audits and any additional requirements associated with the new incentives outlined in the Notice. The incentive approaches proposed can potentially encourage significant improvements in the resilience of the electric sector, however the incentives should in no way influence the scope of a CIP regulatory audit approach. A "Zero Deficiency" incentive plan that also expands the scope of regulatory audits will not be successful.
- **Flexibility in recategorizing expenditures to include workforce development and management.** The approach to incentives in the Notice should include methods to recategorize non-capital expenditures to provide benefits for traditional cybersecurity projects, including workforce development and training. This should also include measurable improvements to the cybersecurity workforce, such as sector-specific security certifications. The ability to treat traditional labor or expense dollars as capital expenditures recoverable under this incentive plan could be a significant capability for entities. The ability to leverage incentive plan elements to pursue cybersecurity tasks associated with programs focused on asset inventory, configuration validations, configuration changes to implement improved cybersecurity controls, and workforce development opportunities would help the industry.
- **Transparent metrics need to be established for qualification of the cybersecurity incentives.** Measuring cybersecurity improvement and efficiency is a challenging research topic within industry, and not limited to just the electric sector. Cybersecurity capabilities are a combination of technology, processes, and workforce development—each with their own unique measures for success. While the

Agenda


Incident Response
Supply Chain
Virtualization
Control Center Comms
Executive Orders

The Virtualization Effort You May be Remembering……

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2016-02 Modifications to CIP Standards
Concepts for Virtualization and Definitions

Do not use this form for submitting comments. Standards Balloting and Commenting System (SBS) to submit comments on **Project 2016-02 Modifications to CIP Standards Virtualization in the CIP Environment.** The electronic form must be submitted by **8 p.m. Eastern, Thursday, November 2, 2017.**

Additional information is available on the project page. If you have questions, contact Katherine Street (404) 446-9702 or Mat Bunch (404) 446-9785.

Background Information

The Standard Drafting Team (SDT) for Project 2016-02 Modifications to CIP Standards continues to work to address transferred issues from the Version 5 Transition Advisory Group (V5 TAG). The V5 TAG consisted of six volunteer Responsible Entities who worked with NERC and the Regional Entities to implement the CIP Version 5 standards in an accelerated time frame. During the implementation study, study participants focused on the technical solutions and processes needed to meet the standards. As a result of this effort, issues were identified with the definition of Cyber Asset as well as the use of virtualization. These issues were documented in CIP V5 Issues for Standard Drafting Team Consideration.

The SDT has conducted outreach to industry on the concepts of virtualization through webinars that are published on the Project 2016-02 Modifications to CIP Standards related files page. To address the topics of the Cyber Asset definition and virtualization, the SDT has developed concepts for which we are seeking informal comment to gather further input from stakeholders. In reviewing these concepts and risks, it became clear that other areas may need to be adjusted to provide a clearer categorization of assets and applicable requirements to address the risk of virtualization.

- ❑ Started almost five years ago
- ❑ Unofficial comment request Nov 2017
- ❑ Definitions
  - ❑ Cyber Asset
  - ❑ Centralized Management Systems (CMS)
  - ❑ Electronic Security Zone (ESZ)
  - ❑ Modify EACMS
  - ❑ Electronic Access Control System (EACS)
  - ❑ Electronic Access Gateway (EAG)
  - ❑ Modify BES Cyber System Information (BES CSI)
- ❑ Standards requirement changes in CIP-004, CIP-005, CIP-006, CIP-007, CIP-009, CIP-010, and CIP-011

Virtualization Activity in Sept 2019 CIP-005-7 – Standard & Definition Draft

Modified	BES Cyber Asset, Transient Cyber Asset, Physical Access Control Systems, Protected Cyber Asset, Intermediate Systems, External Routable Connectivity, Interactive Remote Access, Physical Security Perimeter, Removable Media
Added	Shared Cyber Infrastructure, Virtual Cyber Asset, Physical Access Monitoring Systems, Electronic Access Control System, Electronic Access Monitoring Systems, Electronic Security Zone,
Retired	Electronic Access Point, Electronic Access Control or Monitoring Systems,

Consideration of Comments, Actions, and Ongoing Activities

Virtualization and Future Technologies

Project 2016-02 Standards Drafting Team:
The Case for Change

April 2019

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP Virtualization

Project 2016-02 – CIP Modifications

CIP SDT Members
March, 2020

RELIABILITY | ACCOUNTABILITY

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Virtualization and Future Technologies

Project 2016-02 Standards Drafting Team:
What's in it for me?

April 2020

RELIABILITY | RESILIENCE | SECURITY

Get Connected, Give Back, Guide the Industry

Project 2016-02 Modifications to CIP Standards Related Files

Team Roster

Related Files

File	Size	Date	
Zip File Acrobat Recording	1 MB 8.5 MB	09/28/20 10/01/20	Virtualization Workshop - September 30, 2020 Materials Slides Recording
Acrobat Recording	2 MB	08/18/20	Management Systems - Industry Webinar - August 6, 2020 Slides Recording
Acrobat Acrobat	178 KB 176 KB	07/27/20	Drafting Team Meeting - July 22, 2020 Notes Agenda
Acrobat Recording	492 KB	07/21/20	SuperESP - Industry Webinar - July 2, 2020 Slides Recording
Acrobat	465 KB	06/15/20	Virtualization Overview - ReliabilityFirst Compliance Open Meeting - June 15, 2020 Slides
Acrobat Recording	984 KB	06/15/20	Virtual Machines and Containers - Industry Webinar - June 11, 2020 Slides Recording
Acrobat Recording	964 KB	06/15/20	Hypervisor and Storage Systems - Industry Webinar - May 28, 2020 Slides Recording

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

JDCHRISTOPHER@DRAGOS.COM
@JDCHRISTOPHER

TCONWAY@SANS.ORG
@SANSICS

NERC CIP RELIABILITY STANDARDS

CONTINUOUS IMPLEMENTATION PROJECT OR CHANGE INDUCED PANIC?