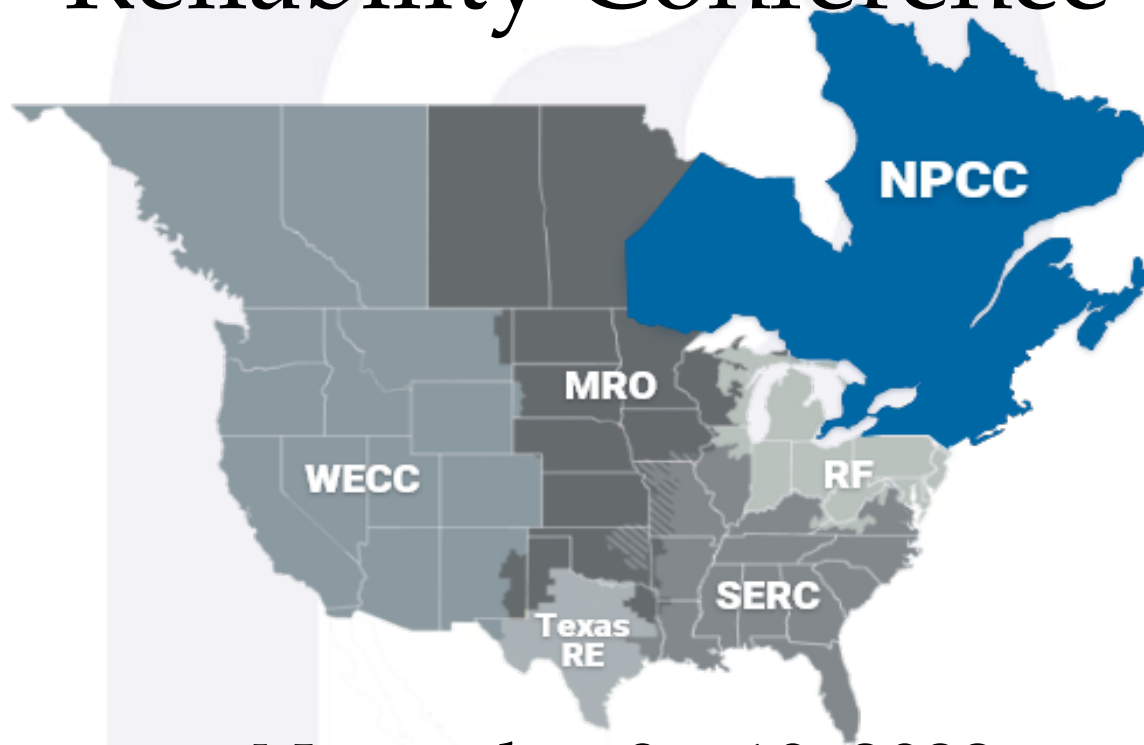


Welcome NPCC Fall 2022 Compliance and Reliability Conference



November 9 – 10, 2022

Disclaimer

The information provided today at this workshop is intended to provide accurate and helpful guidance and education to industry and interested stakeholders. The information provided in this workshop is nonbinding and should not be relied upon for compliance or for other matters. The governing documents for compliance and other matters include the applicable NERC Reliability Standard, NERC Rules of Procedure, various regulatory agency orders, approved Implementation guidance and other laws, rules, and regulations. Compliance with Reliability Standards ultimately depends on the facts and circumstances, quality of evidence, and the language of the Reliability Standard.

Safety Message



NPCC, Inc.

In-person note

There will not be a formal health screen.

- If you are experiencing any symptoms commonly associated with COVID-19 before traveling to the conference, please adjust your plans to make use of the virtual option via Webex.
- If you experience any symptoms commonly associated with COVID-19 after arriving at the conference, we request that you please make use of the virtual option via Webex instead of coming into the ballroom.
- Masks will be optional at the conference, but we welcome attendees to wear one if that makes them feel most comfortable.

Opening Remarks

Charles Dickerson

President and CEO



NPCC Strategic Focus Areas

- Enhancing System Resilience and Assuring Energy Sufficiency
- Reliably Integrating the Resources brought forward by Societal Decarbonization Objectives (DER, VER, Renewables)
- Addressing Cyber and Physical Threats

2023 ERO Compliance Monitoring and Enforcement Program (CMEP) Implementation Plan (IP)

Ben Eng

Manager, Entity Risk Assessment

Implementation Plan Background

Purpose of the CMEP IP

- Annual operating plan for NERC and Regional Entities
- Address risks that will be priorities for ERO Enterprise CMEP activities

Timeline

- Task Force begins IP development in 3rd quarter of preceding year.
- NERC posts final IP with links to Regional schedules in November
- Updates may occur throughout year

CMEP IP Development

Risk Elements

Data-driven and expert judgement of ERO Enterprise staff

Input from ERO Enterprise publications (RISC Report, LTRA)

Identify and prioritize continent-wide, interconnection and regional, risks to the reliability of the bulk power system

Not intended to be a representation of all important Reliability Standard requirements

CMEP IP Intended Use

CMEP staff intended use

- Focus compliance monitoring and enforcement activities
- Messaging to industry on areas of emphasis for CMEP activities

Registered entity intended use

- Used in conjunction with entity-specific COP
- Consideration in compliance operations focus
- Enhance internal controls

2023 CMEP IP Highlights

Focused Message

- Continue emphasis on providing focus and offering usability
- No more Regional specific IPs

Risk Elements reflect a combined ERO Enterprise view

- Focused to increase relevance to impacted registered entities
- Reflects high level priorities for CMEP
- Relevance based on registered entity's facts and circumstances

2022 COVID-19 industry guidance and prioritization

- Removed from 2023 CMEP IP

More ERO Risk Elements, Less Focus Areas

Risk Elements Comparison

Table 1: 2022 Risk Elements

Remote Connectivity
Supply Chain
Models Impacting Long-term and Operational Planning
Gaps in Program Execution
Protection System Coordination
Extreme Events

Table 2: 2023 Risk Elements

Remote Connectivity
Supply Chain
Incident Response
Stability Studies
Inverter-Based Resources
Facility Ratings
Cold Weather Response

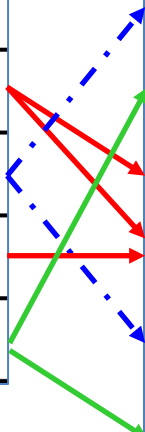
Risk Elements Comparison

Table 1: 2022 Risk Elements

Remote Connectivity
Supply Chain
Models Impacting Long-term and Operational Planning
Gaps in Program Execution
Protection System Coordination
Extreme Events

Table 2: 2023 Risk Elements

Remote Connectivity
Supply Chain
Incident Response
Stability Studies
Inverter-Based Resources
Facility Ratings
Cold Weather Response



Areas of Focus

Incident Response

Incident response has increasingly emerged as a risk to the BPS. Dragos has published a white paper²² on the malware developed by threat group Chernovite named Pipedream. This particular piece of malware is targeting industrial control systems, including the electric sector. One of the long-term readiness best practices within this white paper is to have an updated industrial control system-focused incident response plan with accompanying Standard Operating Procedures and Emergency Operating Procedures for operating with a hampered or degraded control system. Additionally, the CISA Cross-Sector CPGs Common Baseline includes the need to develop, maintain, and practice incident response plans to ensure effective response to threat actions against all assets, along with reporting cybersecurity incidents across IT and OT assets to CISA and any other mandatory reporting stakeholders.

Area of Focus

Table 5: Incident Response				
Focused Risk	Standard	Req	Entities for	Asset Types
Mitigate risks to the reliable operation of the BES as the result of a Cyber Security Incident.	CIP-008-6	R1 R2	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner	Backup Control Centers Control Centers Data Centers Generation Facilities Transmission Facilities Substations

Areas of Focus

Cold Weather Response

Cold weather events encompass a wide range of situations that can cause major BPS impacts. As identified in the 2021 RISC report,³⁴ recent cold weather events (e.g., in ERCOT, MISO, and SPP) show that not only do cold weather events pose challenges due to the nature and frequency of the events themselves, but also that grid transformation heightens the effects and complicates mitigation of the event. Cold weather events can stress the BPS and expose weaknesses such as poor coordination between neighboring entities in planning or operations.

This risk element needs to be understood in light of: the recently expedited FERC approval³⁵ of the Cold Weather Reliability Standards,³⁶ the November 2021 release of the FERC - NERC - Regional Entity Staff Report: The February 2021 Cold Weather Outages in Texas and the South Central United States,³⁷ and the Cold Weather Preparations for Extreme Weather³⁸ Events Alert.³⁹ The updated Reliability Standards changed to focus on cold weather preparedness are not enforceable until April 1, 2023. Therefore, ERO Enterprise CMEP staff may find that an entity has yet to develop and implement the relevant processes and procedures. However, it is important to understand entity plans for, and progress toward, mitigating risk for the upcoming winter and going forward. The ERO Enterprise has developed a Practice Guide⁴⁰ to support understanding of this risk.

Areas of Focus

Table 9: Cold Weather Response			
Rationale	Standard	Requirements	Entities for Attention
Ensure plans are developed and implemented to mitigate operating Emergencies	EOP-011-2	R1, R2, R3, R6, R7	Balancing Authority Generator Owner Reliability Coordinator Transmission Operator

Risk Element/Focus Area Comparison

Table 1: 2022 Risk Elements

Remote Connectivity - 2 standards, 2 requirements
Supply Chain - 2 standards, 3 requirements
Models Impacting Planning - 5 standards, 7 requirements
Gaps in Program Execution - 5 standards, 9 requirements
Protection System Coordination - 4 standards, 6 requirements
Extreme Events - 5 standards, 9 requirements

Table 2: 2023 Risk Elements

Remote Connectivity - 2 standards, 2 requirements
Supply Chain - 2 standards, 3 requirements
Incident Response - 1 standard, 2 requirements
Stability Studies - 2 standards, 3 requirements
Inverter-Based Resources - 3 standards, 6 requirements
Facility Ratings - 1 standard, 1 requirement
Cold Weather Response - 1 standard, 5 requirements

2022: 6 Risk Elements,
23 Standards, 36 requirements

2023: 7 Risk Elements
12 Standards, 22 requirements

Resources

- 2023 ERO Enterprise CMEP IP

<https://www.nerc.com/pa/comp/CAOneStopShop/ERO%20CMEP%20Implementation%20Plan%20v1.0%20-%202023.pdf>

For you DIY-ers:

<https://www.nerc.com>; Program Areas & Departments; Compliance & Enforcement; One Stop Shop (CMEP); One Stop Shop (CMEP, Compliance and Enforcement) – Active; Compliance (37); Implementation Plan (4); ERO CMEP Implementation Plan v1.0 - 2023

Questions?



beng@npcc.org

era@npcc.org





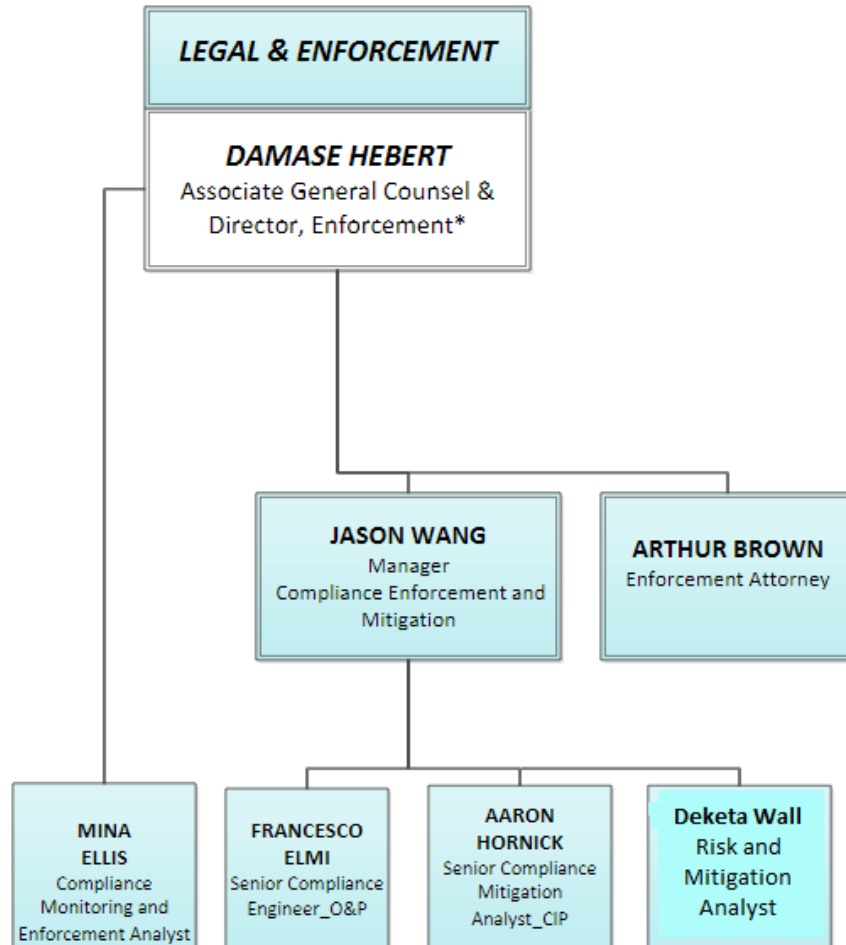
Enforcement Approach

Jason Wang

Manager of Enforcement and
Mitigation



Who is the Enforcement Team and What does Enforcement Do?



- Compliance Exceptions

- Find, Fix, Track

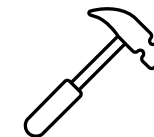


- Spreadsheet Notice of Penalty

- Full Notice of Penalty

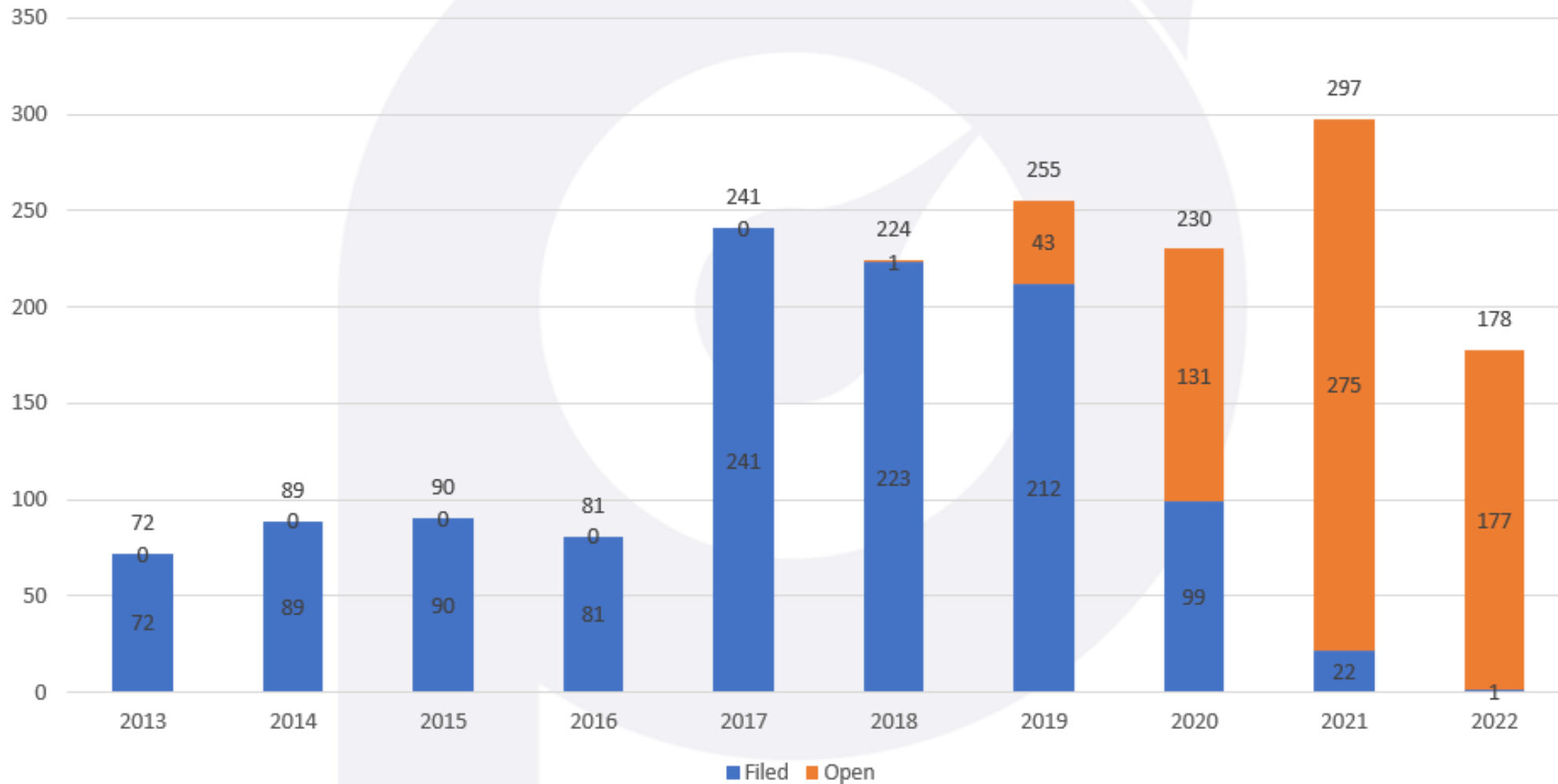


- Mitigation





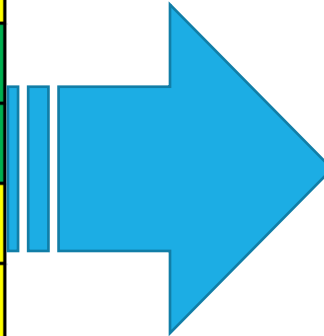
Noncompliance Vintage - Filed/Open





Plan of Action

Standard	Open
CIP-007	84
CIP-010	61
CIP-004	53
MOD-025	38
FAC-008	34
PRC-005	26
CIP-002	21
CIP-006	19
CIP-005	18
CIP-011	16



- Enforcement Approaches

Estimated Completion	Standard	Status
Q1 2022	CIP-006-6 PRC-005-6	Completed
Q2 2022	CIP-007-6 FAC-008-5	Completed
Q3 2022	CIP-002-5.1b CIP-010-2	In Progress



The “What”

- What is an Enforcement Approach?
Standard specific enforcement guidance equivalent to Reliability Standard Audit Worksheet (RSAW).
- What is the Goal?
Provide clear language to help identify reliability violations and standard-specific criteria to evaluate risk



How Are We Going To Do It?

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Home > Program Areas & Departments > Compliance & Enforcement > > Enforcement and Mitigation

Enforcement and Mitigation page provides a consolidated and sortable listing of monthly filings to the Commission for informational purposes only. In the future, this information is expected to be used for enforcement purposes.

Sample Table A

Population Description

Statistical Sampling

Primary Population
(Examples: Substations, Generators, etc.)

Dependent Population
(Examples: etc.)

Example: MOD-025-2 R1 – Identifying Criteria from the Sample

The entity synchronized the Facility on March 29, 2017 and the net active power output identified during commissioning testing was approximately 106 MWs, which is the same value provided by the June 6, 2018 power test.

The Entity owns and operates a single steam turbine generator with nameplate capabilities of 112.5 MW and 132.4 MVA, which interconnect with the host Transmission Owner's BES substation via two 65 MVA generator step-up transformers. In addition, the generator operated at capacity factors of 23.23% in 2017 and 20.82% in 2018.

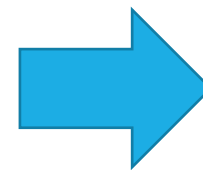
The rated capability of the generator is 5.7% of the Entity's Balancing Authority (NYISO) required Operating Reserve (1965 MW). Therefore, the capacity of this unit can be replaced by the NYISO in the event of an unnecessary trip or loss of generating capability due to inaccurate information.

Previous submittal still reliable

Inherent Properties

Balancing Authority Operating Reserve

General Factors #4...5...6...Etc...



NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

MOD-025-2 Enforcement Approach

Background Information

- [MOD-025-2 Standard Language](#)
- [MOD-025-2 Implementation Plan](#)

Standard/Implementation Plan Effective Dates

- United States

Standard	Requirement	Effective Date	% of Applicable Facilities
MOD-025-2	R1., R2., R3.	07/01/2016	40%
MOD-025-2	R1., R2., R3.	07/01/2017	60%
MOD-025-2	R1., R2., R3.	07/01/2018	80%
MOD-025-2	R1., R2., R3.	07/01/2019	100%

Key Terminology

Applicable Facilities:

- Individual generating unit greater than 20 MVA (gross nameplate rating) directly connected to the Bulk Electric System.
- Synchronous condenser greater than 20 MVA (gross nameplate rating) directly connected to the Bulk Electric System.
- Generating plant/Facility greater than 75 MVA (gross aggregate nameplate rating) directly connected to the Bulk Electric System.

Real Power

The portion of electricity that supplies energy to the load

Reactive Power

The portion of electricity that establishes and sustains the electric and magnetic fields of alternating-current equipment. Reactive Power must be supplied to most types of magnetic equipment, such as motors and transformers. It also must supply the reactive losses on transmission facilities. Reactive Power is provided by generators, synchronous condensers, or electrostatic equipment such as capacitors and directly influences electric system voltage. It is usually expressed in kilovars (kvar) or megavars (Mvar).



Completed Enforcement Approaches

- Operations and Planning
(O&P)

- PRC-005-6
- MOD-025-2
- FAC-008-5

- Cyber Infrastructure Protection
(CIP)

- CIP-004-6
- CIP-006-6
- CIP-007-6



How Risk Criteria was Determined

Step 1: Generalize Risk Statements to create a running list of common risk criteria (O&P Example)

The entity synchronized the Facility on March 29, 2017 and the net active power output identified during commissioning testing was approximately 106 MWs, which is the same value provided by the June 6, 2018 power test.



Previous submittal
still reliable

The Entity owns and operates a single steam turbine generator with nameplate capabilities of 112.5 MW and 132.4 MVA, which interconnect with the host Transmission Owner's BES substation via two 65 MVA generator step-up transformers. In addition, the generator operated at capacity factors of 23.23% in 2017 and 20.82% in 2018.



Inherent Properties

The rated capability of the generator is 5.7% of the Entity's Balancing Authority (NYISO) required Operating Reserve (1965 MW). Therefore, the capacity of this unit can be replaced by the NYISO in the event of an unnecessary trip or loss of generating capability due to inaccurate information.



Balancing Authority
Operating Reserve

General Factors
#4...5...6...Etc...



How Risk Criteria was Determined

Step 1: Generalize Risk Statements to create a running list of common risk criteria (CIP Example)

For the first instance, the access was limited to one individual for the PSPs at a generation station containing medium impact BCS.



Identify individuals in scope

The individual who was granted access also had authorized access to the PSPs containing high impact BCS. For the second instance, the individual who was granted access had other approved access to PSPs.



Address type of access/affected assets or information

The individual had completed the required training and a personnel risk assessment (PRA). For the second instance, this individual had completed cyber security training and a PRA, which are not required for BCS access.



Address PRA/Background Check/Training

The issue was discovered through quarterly BCS access reviews, which go beyond the frequency required by the standard and the individual did not utilize the provisioned access during the duration of the issue.



Duration and address how frequently the access was utilized

General Factors
#4...5...6...Etc...



How Risk Criteria was Determined

Step 2: Iterate the process based on the ERO Sampling Guidelines

Sample Table A	
Population Description	Sample Selection
Statistical Sampling	
Primary Population (Examples: Substations, Generating Stations, ESPs, PSPs, CCAs)	Using Statistical Sampling
1-8	Entire population
9 +	8 Samples
Dependent Population of Elements: (Examples: Relays, CCAs, Routers, Firewalls & Other)	Using Statistical Sampling
1-9	All Elements
10-19	9 Samples
20-40	16 Samples
41-100	23 Samples
101-1000	29 Samples
1001 +	33 Samples

Taken from the ERO Sampling Handbook R1.0 (2015)



Complete the Enforcement Approach

Step 3: Apply the criteria and add/remove, as necessary. Include any region-specific nuances



NORTHEAST POWER COORDINATING COUNCIL, INC.

R2 Scoping and Risk Determination

R2. Each TO, GO, and DP that uses performance-based maintenance intervals in its PSMP shall follow the procedure established in PRC-005 Attachment A to establish and maintain its performance-based intervals. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]

Note: all Registered Entities within NPCC utilize time-based maintenance program(s)

PRC-005-6 R2



Future Plans/Goals

Standard	Open
CIP-007	84
CIP-010	61
CIP-004	53
MOD-025	38
FAC-008	34
PRC-005	26
CIP-002	21
CIP-006	19
CIP-005	18
CIP-011	16

- Complete CIP-005-7 and CIP-011-2 in 2023
- Short Term Future Goal
 - Use Enforcement Approaches to gain necessary preliminary information and Triage noncompliance
- Long Term Future Goal
 - Use Standard Specific Enforcement Approach as Self-Report Forms





NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

CIP-004-6 Enforcement Approach

Background Information

- [CIP-004-6 Standard Language](#)
- [CIP-004-6 Implementation Plan](#)

Standard/Implementation Plan Effective Dates

- **United States**

Standard	Requirement	Effective Date
CIP-004-6	R1., R2., R3., R4., R5	07/01/2016

Key Terminology

Applicable Facilities:

Standard Part	Applicable Systems
R1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems
R2.1 R2.2 R2.3	High Impact BES Cyber Systems and their associated EACMS; and PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated EACMS; and PACS
R3.1 R3.2 R3.3 R3.4 R3.5	High Impact BES Cyber Systems and their associated EACMS; and PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated EACMS; and PACS



R4.1 R4.2 R4.3 R4.4	High Impact BES Cyber Systems and their associated EACMS; and PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated EACMS; and PACS
R5.1 R5.2 R5.3	High Impact BES Cyber Systems and their associated EACMS; and PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated EACMS; and PACS
R5.4 R5.5	High Impact BES Cyber Systems and their associated EACMS

High Impact BES Cyber Systems

Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.

Medium Impact BES Cyber Systems

Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.

Medium Impact BES Cyber Systems with External Routable Connectivity

Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.

Electronic Access Control or Monitoring Systems (EACMS)

Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.



NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

Physical Access Control Systems (PACS)

Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

CIP Exceptional Circumstance

A situation that involves or threatens to involve one or more of the following, or similar, conditions that impact safety or BES reliability:

- a risk of injury or death;
- a natural disaster;
- civil unrest;
- an imminent or existing hardware, software, or equipment failure;
- a Cyber Security Incident requiring emergency assistance;
- a response by emergency services; the enactment of a mutual assistance agreement; or
- an impediment of large scale workforce availability.



R1 Scoping and Risk Determination

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-004-6 Table R1

1.1. Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to the BES Cyber Systems.

R1 Scope Evaluation

Noncompliant with R1	Entity failed to have a documented process which includes security awareness
Noncompliant with R1	Entity failed to implement one or more documented processes for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to the BES Cyber Systems.
Noncompliant with R1.1	Entity failed to implement one or more documented security awareness processes at least once each calendar quarter.
Noncompliant with R1.1	Entity's security awareness failed to include: <ul style="list-style-type: none">- Reinforcement of cyber security practices, or- Reinforcement of physical security practices associated with cyber security

R1 Risk Determination

Risk Failure Statement: Noncompliance with CIP-004-6 R1 increases the risk of compromise or misuse due to a lack of cyber security awareness for personnel who have access to affected assets. A failure to stay abreast of current security practices could increase the likelihood of personnel inadvertently using outdated security practices or engaging in activities that pose a heightened security risk.

Risk Criteria

- Individuals in scope
 - Address personnel risk assessment
 - Address cyber security training, including CIP-004-6 R2 training and other training (e.g., state, job, professional, etc.)
 - Type of access
- VRF is lower
- Address actual harm

Tier 3: Major BES Disturbances	Caused or contributed to a major BES disturbance
--------------------------------	--



NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

Tier 2: Moderate Impact	IROL exceeded, BES limit (non-IROL SOL, frequency, voltage, or ACE) exceeded for >30 minutes, BES Facilities tripped unexpectedly, emergency action taken (e.g., reconfiguration, load shed) to mitigate or prevent the impact of the violation, equipment damage, major (>50%) loss of visibility, control, state estimation, or contingency analysis for over 30 minutes
Tier 1: Minor Impact	Observations similar to those in tier 2 but of lesser magnitude, or loss of ability to monitor cybersecurity intrusions.
Tier 0: No Impact	No observed impact.

R1 Mitigation Verification

- The Responsible Entity is not required to document that each quarter's reinforcement was received by each of its authorized personnel. Rather, the Responsible Entity is required to demonstrate that the security awareness reinforcement was communicated to its authorized personnel as a whole, not necessarily individually.



R2 Scoping and Risk Determination

R2. Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in CIP-004-6 Table R2 – Cyber Security Training Program. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning]

R2.1 Training content on:

- 2.1.1. Cyber security policies;
- 2.1.2. Physical access controls;
- 2.1.3. Electronic access controls;
- 2.1.4. The visitor control program;
- 2.1.5. Handling of BES Cyber System Information and its storage;
- 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan;
- 2.1.7. Recovery plans for BES Cyber Systems;
- 2.1.8. Response to Cyber Security Incidents; and
- 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.

R2.1 Scope Evaluation

Noncompliant with R2	Entity's training program content failed to be appropriate to individual roles, functions, or responsibilities
Noncompliant with R2.1	Entity's training program failed to include content on the following: <ul style="list-style-type: none">1. Cyber Security policies;2. Physical access controls;3. Electronic access controls;4. The visitor control program;5. Handling of BES Cyber System Information and its storage;6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan;7. Recovery plans for BES Cyber Systems;8. Response to Cyber Security Incidents; and9. 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.



R2.1 Risk Determination

Risk Failure Statement: Noncompliance with CIP-004-6 R2.1 increases the risk of compromise or misuse due to a poor training program amongst individuals with access to affected assets. Untrained individuals are more likely to misuse access or fail to adhere to best security practices, thereby increasing the threat to the reliability and resilience of the Bulk Power System.

Risk Criteria

- Individuals in scope
 - Address personnel risk assessment
 - Address cyber security training, including partial CIP-004-6 R2.1 training and other training (e.g., state, job, professional, etc.)
 - Type of access
 - History of handling confidential/sensitive information
- Inherent properties of the entity or affected systems
- Training program differences between standard/requirement and actual content
- Address actual harm

Tier 3: Major BES Disturbances	Caused or contributed to a major BES disturbance
Tier 2: Moderate Impact	IROL exceeded, BES limit (non-IROL SOL, frequency, voltage, or ACE) exceeded for >30 minutes, BES Facilities tripped unexpectedly, emergency action taken (e.g., reconfiguration, load shed) to mitigate or prevent the impact of the violation, equipment damage, major (>50%) loss of visibility, control, state estimation, or contingency analysis for over 30 minutes
Tier 1: Minor Impact	Observations similar to those in tier 2 but of lesser magnitude, or loss of ability to monitor cybersecurity intrusions.
Tier 0: No Impact	No observed impact.

R2.1 Mitigation Verification

- The training program(s) must collectively include all nine training elements.
- It is not necessary that all nine training elements be included for the training of each role, function, or responsibility.
- Each role, function, or responsibility must receive training on all appropriate training elements.



R2.2 Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during [CIP Exceptional Circumstances](#).

R2.2 Scope Evaluation

Noncompliant with R2.2	Entity's personnel failed to complete training specified in Part 2.1 prior to being granted electronic and unescorted physical access to applicable Cyber Assets.
Noncompliant with R2.2	If the entity declared and responded to a CIP Exceptional Circumstance , the Entity failed to adhere to the applicable cyber security policies.

R2.2 Risk Determination

Risk Failure Statement: Noncompliance with CIP-004-6 R2.2 increases the risk of compromise or misuse due to a lack of cyber security training prior to granting individuals access to affected assets. Untrained individuals are more likely to misuse access or fail to adhere to best security practices, thereby increasing the threat to the reliability and resilience of the Bulk Power System.

Risk Criteria

- Individuals in scope
 - Address personnel risk assessment
 - Address cyber security training, including partial CIP-004-6 R2.1 training and other training (e.g., state, job, professional, etc.)
 - Type of access
 - History of handling confidential/sensitive information
- Inherent properties of the entity or affected systems
- Electronic and or physical security controls
- Address actual harm

Tier 3: Major BES Disturbances	Caused or contributed to a major BES disturbance
Tier 2: Moderate Impact	IROL exceeded, BES limit (non-IROL SOL, frequency, voltage, or ACE) exceeded for >30 minutes, BES Facilities tripped unexpectedly, emergency action taken (e.g., reconfiguration, load shed) to mitigate or prevent the impact of the violation, equipment damage, major (>50%) loss of visibility, control, state estimation, or contingency analysis for over 30 minutes



NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

Tier 1: Minor Impact	Observations similar to those in tier 2 but of lesser magnitude, or loss of ability to monitor cybersecurity intrusions.
Tier 0: No Impact	No observed impact.

R2.2 Mitigation Verification

- The responsible entity may reference a separate set of documents to demonstrate its response to any requirements impacted by [CIP Exceptional Circumstances](#).



R2.3 Require completion of the training specified in Part 2.1 at least once every 15 calendar months.

R2.3 Scope Evaluation

Noncompliant with R2.3	Entity personnel with authorized electronic access or authorized unescorted physical access to applicable Cyber Assets failed to complete the training specified in Part 2.1 at least once every 15 calendar months.
------------------------	--

R2.3 Risk Determination

Risk Failure Statement: Noncompliance with CIP-004-6 R2.3 increases the likelihood of personnel utilizing outdated or incorrect security practices or engaging in activities that pose a heightened security risk.

Risk Criteria

- Individuals in scope
 - Address personnel risk assessment
 - Address cyber security training, including partial CIP-004-6 R2.1 training and other training (e.g., state, job, professional, etc.)
 - Type of access
 - History of handling confidential/sensitive information
 - Other security awareness activities (regular e-mails, lunch and learns, poster campaigns, etc.)
- Inherent properties of the entity or affected systems
- Electronic and or physical security controls
- Internal control that may have led to discovery
- Address actual harm

Tier 3: Major BES Disturbances	Caused or contributed to a major BES disturbance
Tier 2: Moderate Impact	IROL exceeded, BES limit (non-IROL SOL, frequency, voltage, or ACE) exceeded for >30 minutes, BES Facilities tripped unexpectedly, emergency action taken (e.g., reconfiguration, load shed) to mitigate or prevent the impact of the violation, equipment damage, major (>50%) loss of visibility, control, state estimation, or contingency analysis for over 30 minutes
Tier 1: Minor Impact	Observations similar to those in tier 2 but of lesser magnitude, or loss of ability to monitor cybersecurity intrusions.



NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

Tier 0: No Impact	No observed impact.

R2.3 Mitigation Verification

- None



R3 Scoping and Risk Determination

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in CIP-004-6 Table R3 – Personnel Risk Assessment Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]

R3.1. Process to confirm identity

R3.1 Scope Evaluation

Noncompliant with R3	Entity failed to implement one or more personnel risk assessment programs to attain and retain authorized electronic or unescorted physical access to BES Cyber Systems
Noncompliant with R3.1	Entity failed to implement a process to confirm identity for personnel with authorized electronic access and/or authorized unescorted physical access to Applicable Systems.

R3.1 Risk Determination

Risk Failure Statement: Noncompliance with CIP-004-6 R3.1 could lead to unauthorized and untrusted individuals accessing critical assets and systems, potentially to the detriment of the Bulk Power System.

Risk Criteria

- Individuals in scope
 - Address extent of background check that was conducted
 - Type of access
- Address actual harm

Tier 3: Major BES Disturbances	Caused or contributed to a major BES disturbance
Tier 2: Moderate Impact	IROL exceeded, BES limit (non-IROL SOL, frequency, voltage, or ACE) exceeded for >30 minutes, BES Facilities tripped unexpectedly, emergency action taken (e.g., reconfiguration, load shed) to mitigate or prevent the impact of the violation, equipment damage, major (>50%) loss of visibility, control, state estimation, or contingency analysis for over 30 minutes
Tier 1: Minor Impact	Observations similar to those in tier 2 but of lesser magnitude, or loss of ability to monitor cybersecurity intrusions.



NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

Tier 0: No Impact	No observed impact.
-------------------	---------------------

R3.1 Mitigation Verification

- None The entity failed to perform a seven year criminal history check as part of each personnel risk assessment. Entity failed to include within the seven year criminal history records check, the current residence, and other locations where the subject has resided for six consecutive months or more.



R3.2 Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes:

- 3.2.1 current residence, regardless of duration; and
- 3.2.2 other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more.

If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.

R3.2 Scope Evaluation

Noncompliant with R3.2	The entity failed to perform a seven year criminal history check as part of each personnel risk assessment for personnel with authorized electronic access and/or authorized unescorted physical access to applicable Cyber Systems
Noncompliant with R3.2.1 and/or 3.2.2	Entity failed to include, within the seven year criminal history records check, the current residence, and other locations where the subject has resided for six consecutive months or more.

R3.2 Risk Determination

Risk Failure Statement: Noncompliance with CIP-004-6 R3.1 could lead to unauthorized and untrusted individuals accessing critical assets and systems, potentially to the detriment of the Bulk Power System.

Risk Criteria

- Individuals in scope
 - Address extent of background check that was conducted
 - Type of access
- Address actual harm

Tier 3: Major BES Disturbances	Caused or contributed to a major BES disturbance
Tier 2: Moderate Impact	IROL exceeded, BES limit (non-IROL SOL, frequency, voltage, or ACE) exceeded for >30 minutes, BES Facilities tripped unexpectedly, emergency action taken (e.g., reconfiguration, load shed) to mitigate or prevent the impact of the violation, equipment damage, major (>50%) loss of



NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

	visibility, control, state estimation, or contingency analysis for over 30 minutes
Tier 1: Minor Impact	Observations similar to those in tier 2 but of lesser magnitude, or loss of ability to monitor cybersecurity intrusions.
Tier 0: No Impact	No observed impact.

R3.2 Mitigation Verification

- None



R3.3 Criteria or process to evaluate criminal history records checks for authorizing access.

R3.3 Scope Evaluation

Noncompliant with R3.3	Entity failed to include criteria or a process to evaluate criminal history records checks for authorizing access within personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that.
Noncompliant with R3.3	Entity failed to implement a criteria or process to evaluate criminal history records for authorizing access for personnel with authorized electronic access and/or authorized unescorted physical access to Applicable Systems.

R3.3 Risk Determination

Risk Failure Statement: Noncompliance with CIP-004-6 R3.3 could result in the entity missing valuable information about an individual's criminal history, thereby potentially exposing the entity and Bulk Power System to heightened security risks.

Risk Criteria

- Individuals in scope
 - Address extent of background check that was conducted
 - Type of access
- Address actual harm

Tier 3: Major BES Disturbances	Caused or contributed to a major BES disturbance
Tier 2: Moderate Impact	IROL exceeded, BES limit (non-IROL SOL, frequency, voltage, or ACE) exceeded for >30 minutes, BES Facilities tripped unexpectedly, emergency action taken (e.g., reconfiguration, load shed) to mitigate or prevent the impact of the violation, equipment damage, major (>50%) loss of visibility, control, state estimation, or contingency analysis for over 30 minutes
Tier 1: Minor Impact	Observations similar to those in tier 2 but of lesser magnitude, or loss of ability to monitor cybersecurity intrusions.
Tier 0: No Impact	No observed impact.



NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

R3.3 Mitigation Verification

- None



R3.4 Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.

R3.4 Scope Evaluation

Noncompliant with R3.4	Entity failed to include criteria or a process to evaluate criminal history records checks for contractors or service vendors personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that.
Noncompliant with R3.4	Entity failed to implement a criteria or process to evaluate criminal history records for authorizing access for contractors or service vendors with authorized electronic access and/or authorized unescorted physical access to Applicable Systems.

R3.4 Risk Determination

Risk Failure Statement: Noncompliance with CIP-004-6 R3.4 could result in the entity missing valuable information about a contractor/vendor's criminal history, thereby potentially exposing the entity and Bulk Power System to heightened security risks.

Risk Criteria

- Individuals in scope
 - Address extent of background check that was conducted
 - Type of access
- Address actual harm

Tier 3: Major BES Disturbances	Caused or contributed to a major BES disturbance
Tier 2: Moderate Impact	IROL exceeded, BES limit (non-IROL SOL, frequency, voltage, or ACE) exceeded for >30 minutes, BES Facilities tripped unexpectedly, emergency action taken (e.g., reconfiguration, load shed) to mitigate or prevent the impact of the violation, equipment damage, major (>50%) loss of visibility, control, state estimation, or contingency analysis for over 30 minutes
Tier 1: Minor Impact	Observations similar to those in tier 2 but of lesser magnitude, or loss of ability to monitor cybersecurity intrusions.
Tier 0: No Impact	No observed impact.



NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

--	--

R3.4 Mitigation Verification

- None



R3.5 Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.

R3.5 Scope Evaluation

Noncompliant with R3.5	Entity's process failed to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.
Noncompliant with R3.5	Entity failed to implement a personnel risk assessment process at least once every seven years for personnel with authorized electronic access and/or authorized unescorted physical access to Applicable Systems.

R3.5 Risk Determination

Risk Failure Statement: Noncompliance with CIP-004-6 R3.5 could cause an entity to miss changes in an individual's criminal history, thereby potentially exposing the entity and Bulk Power System to heightened security risks.

Risk Criteria

- Individuals in scope
 - Address extent of background check that was conducted
 - Type of access
- Address actual harm

Tier 3: Major BES Disturbances	Caused or contributed to a major BES disturbance
Tier 2: Moderate Impact	IROL exceeded, BES limit (non-IROL SOL, frequency, voltage, or ACE) exceeded for >30 minutes, BES Facilities tripped unexpectedly, emergency action taken (e.g., reconfiguration, load shed) to mitigate or prevent the impact of the violation, equipment damage, major (>50%) loss of visibility, control, state estimation, or contingency analysis for over 30 minutes
Tier 1: Minor Impact	Observations similar to those in tier 2 but of lesser magnitude, or loss of ability to monitor cybersecurity intrusions.
Tier 0: No Impact	No observed impact.



NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

R3.5 Mitigation Verification

- None



R4 Scoping and Risk Determination

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R4 – Access Management Program. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Same Day Operations].

R4.1. Process to authorize based on need, as determined by the Responsible Entity, except for [CIP Exceptional Circumstances](#):

4.1.1. Electronic access;

4.1.2. Unescorted physical access into a Physical Security Perimeter; and

4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.

R4.1 Scope Evaluation

Noncompliant with R4.1	Entity failed to have a documented process to authorize based on need for electronic access, unescorted physical access into a physical security perimeter, or access to designated storage locations, whether physical or electronic, for BES Cyber System Information.
Noncompliant with R4.1	Entity failed to authorize based on need for electronic access, unescorted physical access into a physical security perimeter, or access to designated storage locations, whether physical or electronic, for BES Cyber System Information.

R4.1 Risk Determination

Risk Failure Statement: Noncompliance with CIP-004-6 R4.1

Risk Criteria

- Individuals in scope
 - Personnel risk assessment/background check
 - Address cyber security training
- Address type of access/affected assets or information
- Address how frequently the access was utilized
- Address whether access was necessary and proper
- Address actual harm

Tier 3: Major BES Disturbances	Caused or contributed to a major BES disturbance
Tier 2: Moderate Impact	IROL exceeded, BES limit (non-IROL SOL, frequency, voltage, or ACE) exceeded for >30 minutes, BES Facilities tripped unexpectedly,



NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

	emergency action taken (e.g., reconfiguration, load shed) to mitigate or prevent the impact of the violation, equipment damage, major (>50%) loss of visibility, control, state estimation, or contingency analysis for over 30 minutes
Tier 1: Minor Impact	Observations similar to those in tier 2 but of lesser magnitude, or loss of ability to monitor cybersecurity intrusions.
Tier 0: No Impact	No observed impact.

R4.1 Mitigation Verification

- The Responsible Entity may reference a separate set of documents to demonstrate its response to any requirements impacted by [CIP Exceptional Circumstances](#).



R4.2. Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.

R4.2 Scope Evaluation

Noncompliant with R4.2	Entity's access management program failed to include a process to verify at least once each calendar quarter that individuals with active electronic or unescorted physical access have authorization records
Noncompliant with R4.2	Entity failed to verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.

R4.2 Risk Determination

Risk Failure Statement: Noncompliance with CIP-004-6 R4.2 could allow an instance of unauthorized access to persist undetected, and such access could be exploited or misused to the detriment of the Bulk Power System.

Risk Criteria

- Scope of issue (e.g., failed to perform entire review or failed to include a specific subset of individuals)
- Individuals in scope
 - Address personnel risk assessment
 - Address training
 - Type of access
 - Working reputation
 - Authorized access to other assets or confidential information (trusted)
- Address actual harm

Tier 3: Major BES Disturbances	Caused or contributed to a major BES disturbance
Tier 2: Moderate Impact	IROL exceeded, BES limit (non-IROL SOL, frequency, voltage, or ACE) exceeded for >30 minutes, BES Facilities tripped unexpectedly, emergency action taken (e.g., reconfiguration, load shed) to mitigate or prevent the impact of the violation, equipment damage, major (>50%) loss of visibility, control, state estimation, or contingency analysis for over 30 minutes
Tier 1: Minor Impact	Observations similar to those in tier 2 but of lesser magnitude, or loss of ability to monitor cybersecurity intrusions.
Tier 0: No Impact	No observed impact.



NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

R4.2 Mitigation Verification

- None



R4.3. For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary

R4.3 Scope Evaluation

Noncompliant with R4.3	Entity failed to verify that all electronic user accounts, user groups, or user role categories and their specific, associated privileges, were correct and determined to be necessary within 15 calendar months.
------------------------	---

R4.3 Risk Determination

Risk Failure Statement: Noncompliance with CIP-004-6 R4.3 could result in an individual retaining unnecessary or overbroad access, which could be exploited or misused to the detriment of the Bulk Power System.

Risk Criteria

- Scope of issue (e.g., failed to perform entire review or failed to include a specific subset of individuals)
- Individuals in scope
 - Address personnel risk assessment
 - Address training
 - Type of access
 - Working reputation
 - Authorized access to other assets or confidential information (trusted)
- Address actual harm

Tier 3: Major BES Disturbances	Caused or contributed to a major BES disturbance
Tier 2: Moderate Impact	IROL exceeded, BES limit (non-IROL SOL, frequency, voltage, or ACE) exceeded for >30 minutes, BES Facilities tripped unexpectedly, emergency action taken (e.g., reconfiguration, load shed) to mitigate or prevent the impact of the violation, equipment damage, major (>50%) loss of visibility, control, state estimation, or contingency analysis for over 30 minutes
Tier 1: Minor Impact	Observations similar to those in tier 2 but of lesser magnitude, or loss of ability to monitor cybersecurity intrusions.
Tier 0: No Impact	No observed impact.



NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

R4.3 Mitigation Verification

- None



R4.4. Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.

R4.4 Scope Evaluation

Noncompliant with R4.4	Entity failed to verify that access to the designated storage locations for BCSI, whether physical or electronic, were correct and determined necessary for performing work functions within 15 calendar months.
------------------------	--

R4.4 Risk Determination

Risk Failure Statement: Noncompliance with CIP-004-6 R4.4 could allow an instance of unauthorized, unnecessary, or overbroad access to persist undetected, and such access could result in the exploitation of misuse of sensitive information.

Risk Criteria

- Information protection controls
 - Monitoring of accounts, folders, files, storage locations
- Type of information
- Individuals in scope
 - Address personnel risk assessment
 - Address training
 - Type of access
 - Working reputation
 - Authorized access to other assets or confidential information (trusted)
- Address actual harm

Tier 3: Major BES Disturbances	Caused or contributed to a major BES disturbance
Tier 2: Moderate Impact	IROL exceeded, BES limit (non-IROL SOL, frequency, voltage, or ACE) exceeded for >30 minutes, BES Facilities tripped unexpectedly, emergency action taken (e.g., reconfiguration, load shed) to mitigate or prevent the impact of the violation, equipment damage, major (>50%) loss of visibility, control, state estimation, or contingency analysis for over 30 minutes
Tier 1: Minor Impact	Observations similar to those in tier 2 but of lesser magnitude, or loss of ability to monitor cybersecurity intrusions.
Tier 0: No Impact	No observed impact.



NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

R4.4 Mitigation Verification

- None



R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R5 – Access Revocation.

R5.1 A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).

R5.1 Scope Evaluation

Noncompliant with R5	Entity failed to implement an access revocation program
Noncompliant with R5.1	Entity failed to implement a process to initiate removal of an individual's ability for unescorted physical access and/or Interactive Remote Access upon a termination action.
Noncompliant with R5.1	Entity failed to complete the removals within 24 hours of a termination action

R5.1 Risk Determination

Risk Failure Statement: Noncompliance with CIP-004-6 R4.4 could result in that access being misused or exploited to the detriment of the Bulk Power System.

Risk Criteria

- Terms and circumstances of separation
 - Voluntarily on good terms
 - Immediate involuntary
- Individuals in scope
 - Type of access
 - Unescorted physical access
 - Interactive Remote Access
 - Background Check
- Factors impacted ability to exploit remaining access that may restrict ability to exploit remaining access. Examples include:
 - Retrieved physical access badge
 - Retrieved entity issued laptop
- Address actual harm

Tier 3: Major BES Disturbances	Caused or contributed to a major BES disturbance
Tier 2: Moderate Impact	IROL exceeded, BES limit (non-IROL SOL, frequency, voltage, or ACE) exceeded for >30 minutes, BES Facilities tripped unexpectedly, emergency action taken (e.g., reconfiguration, load shed) to mitigate or prevent the impact of the



NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

	violation, equipment damage, major (>50%) loss of visibility, control, state estimation, or contingency analysis for over 30 minutes
Tier 1: Minor Impact	Observations similar to those in tier 2 but of lesser magnitude, or loss of ability to monitor cybersecurity intrusions.
Tier 0: No Impact	No observed impact.

R5.1 Mitigation Verification

- None



R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R5 – Access Revocation.

R5.2 For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.

R5.2 Scope Evaluation

Noncompliant with R5	Entity failed to implement an access revocation program
Noncompliant with R5.2	For a reassignment or transfer, the Entity failed to revoke the individual's authorized electronic access to individual accounts and/or authorized unescorted physical access by the end of the next calendar day following the date that the individual no longer requires retention of that access.

R5.2 Risk Determination

Risk Failure Statement: Noncompliance with CIP-004-6 R5.2 could result in such access be exploited or misused to the detriment of the Bulk Power System.

Risk Criteria

- Terms and circumstances of reassignment/transfer
 - Voluntarily on good terms
 - Involuntary demotion
 - Involuntary reassignment
- Individuals in scope
 - Type of access
 - Unescorted physical access
 - Interactive Remote Access
 - Continued access to separate protected systems and confidential information in new role (trusted)
 - Address personnel risk assessment
 - Address training
- Address actual harm

Tier 3: Major BES Disturbances	Caused or contributed to a major BES disturbance
Tier 2: Moderate Impact	IROL exceeded, BES limit (non-IROL SOL, frequency, voltage, or ACE) exceeded for >30 minutes, BES Facilities tripped unexpectedly, emergency action taken (e.g., reconfiguration, load shed) to mitigate or prevent the impact of the



NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

	violation, equipment damage, major (>50%) loss of visibility, control, state estimation, or contingency analysis for over 30 minutes
Tier 1: Minor Impact	Observations similar to those in tier 2 but of lesser magnitude, or loss of ability to monitor cybersecurity intrusions.
Tier 0: No Impact	No observed impact.

R5.2 Mitigation Verification

- None



R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R5 – Access Revocation.

R5.3 For termination actions, revoke the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.

R5.3 Scope Evaluation

Noncompliant with R5	Entity failed to implement an access revocation program
Noncompliant with R5.3	Entity failed to revoke an individual's physical or electronic access to the designated storage locations for BCSI by the end of the next calendar day following the effective date of the termination.

R5.3 Risk Determination

Risk Failure Statement: Noncompliance with CIP-004-6 R5.3 could result in that access being misused or exploited to the detriment of the Bulk Power System.

Risk Criteria

- Terms and circumstances of separation
 - Voluntarily on good terms
 - Immediate involuntary
- Individuals in scope
 - Type of access
 - Unescorted physical access
 - Interactive Remote Access
 - Background Check
- Factors impacted ability to exploit remaining access that may restrict ability to exploit remaining access. Examples include:
 - Retrieved physical access badge
 - Retrieved entity issued laptop
- Address actual harm

Tier 3: Major BES Disturbances	Caused or contributed to a major BES disturbance
Tier 2: Moderate Impact	IROL exceeded, BES limit (non-IROL SOL, frequency, voltage, or ACE) exceeded for >30 minutes, BES Facilities tripped unexpectedly, emergency action taken (e.g., reconfiguration, load shed) to mitigate or prevent the impact of the violation, equipment damage, major (>50%) loss of



NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

	visibility, control, state estimation, or contingency analysis for over 30 minutes
Tier 1: Minor Impact	Observations similar to those in tier 2 but of lesser magnitude, or loss of ability to monitor cybersecurity intrusions.
Tier 0: No Impact	No observed impact.

R5.3 Mitigation Verification

- None



R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R5 – Access Revocation.

R5.4 For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.

R5.4 Scope Evaluation

Noncompliant with R5	Entity failed to implement an access revocation program
Noncompliant with R5.4	Entity failed to revoke the individual's non-shared user accounts within 30 calendar days of the effective date of a termination action.

R5.4 Risk Determination

Risk Failure Statement: Noncompliance with CIP-004-6 R5.4 could result in such access be exploited or misused to the detriment of the Bulk Power System.

Risk Criteria

- Terms and circumstances of reassignment/transfer
 - Voluntarily on good terms
 - Involuntary demotion
 - Involuntary reassignment
- Account(s) in scope
 - Purpose of the account
 - Function of the account
 - Privileges of the affected accounts
- Individual(s) in scope
 - Background check
- Factors impacted ability to exploit remaining access that may restrict ability to exploit remaining access. Examples include:
 - Retrieved physical access badge
 - Retrieved entity issued laptop
- Address actual harm

Tier 3: Major BES Disturbances	Caused or contributed to a major BES disturbance
Tier 2: Moderate Impact	IROL exceeded, BES limit (non-IROL SOL, frequency, voltage, or ACE) exceeded for >30 minutes, BES Facilities tripped unexpectedly, emergency action taken (e.g., reconfiguration, load shed) to mitigate or prevent the impact of the violation, equipment damage, major (>50%) loss of



NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

	visibility, control, state estimation, or contingency analysis for over 30 minutes
Tier 1: Minor Impact	Observations similar to those in tier 2 but of lesser magnitude, or loss of ability to monitor cybersecurity intrusions.
Tier 0: No Impact	No observed impact.

R5.4 Mitigation Verification

- None



R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R5 – Access Revocation.

R5.5 For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.

R5.5 Scope Evaluation

Noncompliant with R5	Entity failed to implement an access revocation program
R5.5	For a termination action, the Entity failed to change passwords for shared account(s) known to the user within 30 calendar days of the termination action.
Noncompliant with R5.5	For a reassignment or transfer, the Entity failed to change passwords for shared account(s) known to the user within 30 calendar days following the date the individual no longer requires retention of that access.
Noncompliant with R5.5	For extenuating operating circumstances, the Entity failed to change the password(s) within 10 calendar days following the end of the operating circumstances.

R5.5 Risk Determination

Risk Failure Statement: Noncompliance with CIP-004-6 R5.5 could result in an individual exploiting known shared account passwords to the detriment of the Bulk Power System.

Risk Criteria

- Reassignment/Transfer
 - Terms and circumstances
 - Voluntarily on good terms
 - Involuntary demotion
 - Involuntary reassignment
 - Individuals in scope
 - Background
 - Continued access to separate protected systems and confidential information in new role (trusted)
- Termination Action
 - Terms and circumstances
 - Voluntarily on good terms
 - Immediate involuntary



NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

- Individuals in scope
 - Background Check
- Factors impacted ability to exploit remaining access that may restrict ability to exploit remaining access. Examples include:
 - Retrieved physical access badge
 - Retrieved entity issued laptop
- Address actual harm

Tier 3: Major BES Disturbances	Caused or contributed to a major BES disturbance
Tier 2: Moderate Impact	IROL exceeded, BES limit (non-IROL SOL, frequency, voltage, or ACE) exceeded for >30 minutes, BES Facilities tripped unexpectedly, emergency action taken (e.g., reconfiguration, load shed) to mitigate or prevent the impact of the violation, equipment damage, major (>50%) loss of visibility, control, state estimation, or contingency analysis for over 30 minutes
Tier 1: Minor Impact	Observations similar to those in tier 2 but of lesser magnitude, or loss of ability to monitor cybersecurity intrusions.
Tier 0: No Impact	No observed impact.

R5.5 Mitigation Verification

- None

NPCC Specific Details

- None

Enforcement Notes

- None



CIP-006-6 Enforcement Approach

Background Information

- [CIP-006-6 Standard Language](#)
- [CIP-006-6 Implementation Plan](#)

Standard/Implementation Plan Effective Dates

- **United States**

Standard	Requirement	Effective Date
CIP-006-6	R1., R2., R3.	07/01/2016
CIP-006-6	R1.10	04/01/2017

Key Terminology

High Impact BES Cyber Systems

Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.

Medium Impact BES Cyber Systems

Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.

Medium Impact BES Cyber Systems without External Routable Connectivity

Only applies to medium impact BES Cyber Systems without External Routable Connectivity.

Medium Impact BES Cyber Systems with External Routable Connectivity

Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.

Electronic Access Control or Monitoring Systems (EACMS)

Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.



NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

Physical Access Control Systems (PACS)

Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

Protected Cyber Assets (PCA)

Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

Locally mounted hardware or devices at the Physical Security Perimeter

Applies to the locally mounted hardware or devices (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) at a Physical Security Perimeter associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity, and that does not contain or store access control information or independently perform access authentication. These hardware and devices are excluded in the definition of Physical Access Control Systems.

CIP Exceptional Circumstance

A situation that involves or threatens to involve one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death; a natural disaster; civil unrest; an imminent or existing hardware, software, or equipment failure; a Cyber Security Incident requiring emergency assistance; a response by emergency services; the enactment of a mutual assistance agreement; or an impediment of large scale workforce availability.



R1 Scoping and Risk Determination

R1. Each Responsible Entity shall implement one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in CIP-006-6 Table R1 – Physical Security Plan.

- 1.1. Define operational or procedural controls to restrict physical access
- 1.2. Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.
- 1.3. Where technically feasible, utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access.
- 1.4. Monitor for unauthorized access through a physical access point into a Physical Security Perimeter.
- 1.5. Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.
- 1.6. Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.
- 1.7. Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.
- 1.8. Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry.
- 1.9. Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days.
- 1.10. Restrict physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter.

Where physical access restrictions to such cabling and components are not implemented, the Responsible Entity shall document and implement one or more of the following:

- encryption of data that transits such cabling and components; or



NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

- 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.

R1 Scope Evaluation

- How long were there no controls to restrict physical access?
- What type of assets became vulnerable to unauthorized physical access?
- What were the assets responsible for?
- How many individuals gained unauthorized access?
- How many access points were affected?
- Specify which part was noncompliant

Noncompliant with R1.1	Entity failed to define operational or procedural controls to restrict physical access
Noncompliant with R1.2	Entity failed to use at least one physical access control to allow only those with authorized unescorted access into each PSP
Noncompliant with R1.3	Entity failed to use two or more different physical access controls to allow unescorted physical access into the PSP for only those with unescorted physical access.
Noncompliant with R1.4	Entity failed to monitor for unauthorized access through a physical access point into a PSP.
Noncompliant with R1.5	Entity failed to issue an alarm in response to a detected unauthorized access through a physical access point into a PSP within 15 minutes of detection.
Noncompliant with R1.6	Entity failed to monitor each Physical Access Control System (PACS) for unauthorized physical access to a PACS.
Noncompliant with R1.7	Entity failed to issue an alarm in response to detected unauthorized physical access to a PACS to the personnel identified in the BCSI response plan within 15 minutes of detection.
Noncompliant with R1.8	Entity failed to log entity of each individual with unescorted physical access into a PSP with information to identify the date and time of entry.



Noncompliant with R1.9	Entity failed to retain physical access log of entry of individuals with authorized unescorted physical access into a PSP for at least 90 days.
Noncompliant with R1.10	Entity failed to restrict physical access to cabling and other nonprogrammable communication components use for connection between Cyber Assets within the ESP when cabling and components are located outside of the PSP. Entity failed to implement encryption of data that transits such cabling and components.
Noncompliant with R1.10	Entity failed to monitor the status of the communication link and issue an alarm within 15 minutes of a detected issue.
Noncompliant with R1.10	Entity failed to monitor the status of the communication link.
Noncompliant with R1.10	Entity failed to implement an equally effective logical protection.

R1.1 Risk Determination

Risk Failure Statement: Noncompliance with CIP-006-6 R1. increases the likelihood of unauthorized personnel entering a Physical Security Perimeter (PSP).

Risk Criteria

- Identify the other physical protections of the facility:
 - PSP – Is there an otherwise secured outer perimeter?
 - What other physical protections are in place? Do they include:
 - Card Access
 - Guards Monitoring
 - Fences and Locked Gates
 - Intrusion Alarms
 - Is there external or internal video surveillance?
- Are there secured areas for specific Cyber Assets that may be at risk?
- How many access points were affected?
- Supporting electronic protections
 - Is there an Intrusion Detection System (IDS)?
 - Are the assets in scope capable of logging?
 - Is there other electronic monitoring or alarming?
- Establish the duration of the noncompliance
- Did anyone unauthorized gain access?
- What was the BES Impact Categorization?
- Address actual harm



R1.2 Risk Determination

Risk Failure Statement: Noncompliance with CIP-006-6 R1.2 increases the likelihood of unauthorized personnel entering a Physical Security Perimeter (PSP).

Risk Criteria

- Identify the other physical protections of the facility:
 - PSP – Is there an otherwise secured outer perimeter?
 - What other physical protections are in place? Do they include:
 - Card Access
 - Guards Monitoring
 - Can guards respond quickly?
 - Fences and Locked Gates
 - Intrusion Alarms – Forced Door Alarms
 - Video Surveillance / Thermal Cameras / Motion Detectors
- Are there secured areas for specific Cyber Assets that may be at risk?
- Is there perimeter or internal video surveillance?
- Supporting electronic protections on assets in scope:
 - Is there an Intrusion Detection System (IDS)?
 - Are the assets in scope capable of logging?
 - Is there other electronic monitoring or alarming?
- Establish the duration of the noncompliance
- Did anyone unauthorized gain access?
- Were there any unique factors?
- What was the BES Impact Categorization?
- Address actual harm

R1.3 Risk Determination

Risk Failure Statement: Noncompliance with CIP-006-6 R1.3 increases the likelihood of unauthorized personnel gaining physical access to a Physical Security Perimeter (PSP).

Risk Criteria

- Identify the other physical protections of the facility:
 - PSP – Is there an otherwise secured outer perimeter?
 - What other physical protections are in place? Do they include:
 - Card Access
 - Guards Monitoring
 - Fences and Locked Gates
 - Intrusion Alarms – Forced Door Alarms
 - Video Surveillance / Thermal Cameras / Motion Detectors
- Are there secured areas for specific Cyber Assets that may be at risk?



NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

- Is there perimeter or internal video surveillance?
- Supporting electronic protections on assets in scope:
 - Is there an Intrusion Detection System (IDS)?
 - Are the assets in scope capable of logging?
 - Is there other electronic monitoring or alarming?
 - Did assets in scope have port blockers?
- Establish the duration of the noncompliance
- Did anyone unauthorized gain access?
- If someone did gain physical access,
 - How many gained access?
 - How long were did the unauthorized have access?
 - Did they have any under qualifications that provided some level of trust in the personnel? (Personnel Risk Assessments, CIP Training, Long-Trusted Employees)
- Were there any unique factors?
- What was the BES Impact Categorization?
- Address actual harm

R1.4 Risk Determination

Risk Failure Statement: Noncompliance with CIP-006-6 R1.4 increases the likelihood of unauthorized personnel gaining physical access to a Physical Security Perimeter (PSP).

Risk Criteria

- Identify the other physical protections of the facility:
 - PSP – Is there an otherwise secured outer perimeter?
 - What other physical protections are in place? Do they include:
 - Card Access
 - Guards Monitoring
 - Fences and Locked Gates
 - Intrusion Alarms – Forced Door Alarms
 - Video Surveillance / Thermal Cameras / Motion Detectors
- Are there secured areas for specific Cyber Assets that may be at risk?
- Is there perimeter or internal video surveillance?
- Supporting electronic protections on assets in scope:
 - Is there an Intrusion Detection System (IDS)?
 - Are the assets in scope capable of logging?
 - Is there other electronic monitoring or alarming?
- Establish the duration of the noncompliance
- Did anyone unauthorized gain access?
- If someone did gain physical access,
 - How many gained access?
 - How long were did the unauthorized have access?



NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

- Did they have any under qualifications that provided some level of trust in the personnel? (Personnel Risk Assessments, CIP Training, Long-Trusted Employees)
- Were there any unique factors?
- What was the BES Impact Categorization?
- Address actual harm

R1.5 Risk Determination

Risk Failure Statement: Noncompliance with CIP-006-6 R1.5 increases the likelihood of unauthorized personnel gaining undetected physical access to a Physical Security Perimeter (PSP).

Risk Criteria

- Identify the other physical protections of the facility:
 - PSP – Is there an otherwise secured outer perimeter?
 - What other physical protections are in place? Do they include:
 - Card Access
 - Guards Monitoring
 - Fences and Locked Gates
 - Video Surveillance / Thermal Cameras / Motion Detectors
 - Physical Access Logging
- Are there secured areas for specific Cyber Assets that may be at risk?
- Is there perimeter or internal video surveillance?
- Supporting electronic protections on assets in scope:
 - Is there an Intrusion Detection System (IDS)?
 - Are the assets in scope capable of logging?
 - Is there other electronic monitoring or alarming?
- Establish the duration of the noncompliance
- Did anyone unauthorized gain access?
- If someone did gain physical access,
 - How many gained access?
 - How long were did the unauthorized have access?
 - Did they have any under qualifications that provided some level of trust in the personnel? (Personnel Risk Assessments, CIP Training, Long-Trusted Employees)
- Were there any unique factors?
- What was the BES Impact Categorization?
- Address actual harm

R1.6 Risk Determination



Risk Failure Statement: Noncompliance with CIP-006-6 R1.6 increases the likelihood of unauthorized personnel gaining physical access to a Physical Access Control System (PACS).

Risk Criteria

- Identify the other physical protections of the facility:
 - PSP – Is there an otherwise secured outer perimeter?
 - What other physical protections are in place? Do they include:
 - Card Access
 - Guards Monitoring – Is the location manned at all times?
 - Fences and Locked Gates
 - Video Surveillance / Thermal Cameras / Motion Detectors
 - Physical Access Logging
- Are there secured areas for specific Cyber Assets that may be at risk?
- Is there perimeter or internal video surveillance?
- Supporting electronic protections on assets in scope:
 - Is there an Intrusion Detection System (IDS)?
 - Are the assets in scope capable of logging?
 - Is there other electronic monitoring or alarming?
- Establish the duration of the noncompliance
- Did anyone unauthorized gain access?
- If someone did gain physical access,
 - How many gained access?
 - How long were did the unauthorized have access?
 - Did they have any under qualifications that provided some level of trust in the personnel? (Personnel Risk Assessments, CIP Training, Long-Trusted Employees)
- Were there any unique factors?
- What was the BES Impact Categorization?
- Address actual harm

R1.7 Risk Determination

Risk Failure Statement: Noncompliance with CIP-006-6 R1.7 increases the likelihood of unauthorized personnel gaining physical access to a Physical Security Perimeter (PSP) and Physical Access Control System (PACS).

Risk Criteria

- Identify the other physical protections of the facility:
 - PSP – Is there an otherwise secured outer perimeter?
 - What other physical protections are in place? Do they include:
 - Card Access
 - Guards Monitoring – Is the location manned at all times?
 - Fences and Locked Gates
 - Video Surveillance / Thermal Cameras / Motion Detectors
 - Physical Access Logging



NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

- Are there secured areas for specific Cyber Assets that may be at risk?
- Is there perimeter or internal video surveillance?
- Supporting electronic protections on assets in scope:
 - Is there an Intrusion Detection System (IDS)?
 - Are the assets in scope capable of logging?
 - Is there other electronic monitoring or alarming?
- Establish the duration of the noncompliance
- Did anyone unauthorized gain access?
- If someone did gain physical access,
 - How many gained access?
 - How long were did the unauthorized have access?
 - Did they have any under qualifications that provided some level of trust in the personnel? (Personnel Risk Assessments, CIP Training, Long-Trusted Employees)
- Were there any unique factors?
- What was the BES Impact Categorization?
- Address actual harm

R1.8 Risk Determination

Risk Failure Statement: Noncompliance with CIP-006-6 R1.8 reduces the ability of an entity to investigate after a Cyber Security event resulting from unauthorized physical access.

Risk Criteria

- Identify the other physical protections of the facility:
 - PSP – Is there an otherwise secured outer perimeter?
 - What other physical protections are in place? Do they include:
 - Card Access
 - Guards Monitoring – Is the location manned at all times?
 - Fences and Locked Gates
 - Video Surveillance / Thermal Cameras / Motion Detectors
 - Logging by other means?
- Are there secured areas for specific Cyber Assets that may be at risk?
- Is there perimeter or internal video surveillance?
- Supporting electronic protections on assets in scope:
 - Is there an Intrusion Detection System (IDS)?
 - Are the assets in scope capable of logging?
 - Is there other electronic monitoring or alarming?
- Establish the duration of the noncompliance
- Did anyone unauthorized gain access?
- If someone did gain physical access,
 - How many gained access?
 - How long were did the unauthorized have access?



NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

- Did they have any under qualifications that provided some level of trust in the personnel? (Personnel Risk Assessments, CIP Training, Long-Trusted Employees)
- Were there any unique factors?
- What was the BES Impact Categorization?
- Address actual harm

R1.9 Risk Determination

Risk Failure Statement: Noncompliance with CIP-006-6 R1.9 reduces the ability of an entity to investigate after a Cyber Security event resulting from unauthorized physical access.

Risk Criteria

- Identify the other physical protections of the facility:
 - PSP – Is there an otherwise secured outer perimeter?
 - What other physical protections are in place? Do they include:
 - Card Access
 - Guards Monitoring – Is the location manned at all times?
 - Fences and Locked Gates
 - Video Surveillance / Thermal Cameras / Motion Detectors
 - Logging by other means?
- Are there secured areas for specific Cyber Assets that may be at risk?
- Is there perimeter or internal video surveillance?
- Supporting electronic protections on assets in scope:
 - Is there an Intrusion Detection System (IDS)?
 - Are the assets in scope capable of logging?
 - Is there other electronic monitoring or alarming?
- Establish the duration of the noncompliance
- Did anyone unauthorized gain access?
- If someone did gain physical access,
 - How many gained access?
 - How long were did the unauthorized have access?
 - Did they have any under qualifications that provided some level of trust in the personnel? (Personnel Risk Assessments, CIP Training, Long-Trusted Employees)
- Were there any unique factors?
- What was the BES Impact Categorization?
- Address actual harm

R1.10 Risk Determination



Risk Failure Statement: Noncompliance with CIP-006-6 R1.10 increases the likelihood of unauthorized personnel gaining access and potentially tampering with cabling and other communication components used between Cyber Assets within the same ESP where cabling is located outside the PSP without detection by the entity.

Risk Criteria

- Identify the other physical protections of the facility:
 - PSP – Is there an otherwise secured outer perimeter?
 - Are there cabling specific physical protections?
 - Is the cabling within the interior of another building or other physically secured area?
 - Was access to the cabling limited?
 - Was armored fiber optic cabling employed?
 - Are there other physical protections in place? Do they include:
 - Cabling on the interior portion of a building?
 - Card Access
 - Guards Monitoring – Is the location manned at all times?
 - Fences and Locked Gates
 - Video Surveillance / Thermal Cameras / Motion Detectors
- Were there supporting electronic protections on assets in scope:
 - Is there an Intrusion Detection System (IDS)?
 - Are the assets in scope capable of logging?
 - Is there other electronic monitoring or alarming?
- Establish the duration of the noncompliance
- Was the issue primarily one of documentation?
- Did anyone unauthorized gain access?
- If someone did gain physical access,
 - How many gained access?
 - How long were did the unauthorized have access?
 - Did they have any under qualifications that provided some level of trust in the personnel? (Personnel Risk Assessments, CIP Training, Long-Trusted Employees)
- Were there any unique factors?
- What was the BES Impact Categorization?
- Address actual harm

R1 Mitigation Verification

- For Verification Check
 - Are there process documents that discuss the operational or procedural controls to restrict physical access?
 - Are there change control documents that show the implementation of physical access controls?
 - Are there records of alarms or alerts issued in response to unauthorized entry into a PSP?



NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

- Are there email records of actions completed? Do they align with the timelines provided?
- Are there pictures of signage posted?
- Are there sign in sheets, emails, or other digital evidence of training or awareness notifications.
- Has the entity provided digital logs or sign in sheets for entry into the PSP?



R2 Scoping and Risk Determination

R2. Each Responsible Entity shall implement one or more documented visitor control program(s) that include each of the applicable requirement parts in CIP-006-6 Table R2 – Visitor Control Program.

2.1. Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter, except during CIP Exceptional Circumstances.

2.2. Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.

2.3. Retain visitor logs for at least ninety calendar days.

R2 Scope Evaluation

- Specify which part was noncompliant

Noncompliant with R2.1	Entity failed to require continuous escorted access of visitors within a PSP.
Noncompliant with R2.2	Entity failed to require manual or automated logging of visitors within a PSP.
Noncompliant with R2.3	Entity failed to retain visitor logs for at least 90 days.

R2 Risk Determination

Risk Failure Statement (2.1): Noncompliance with CIP-006-6 R2 increases the likelihood of an individual gaining unescorted physical access to high or medium impact assets that could be exploited to access, alter, or otherwise harm Cyber Assets.

Risk Failure Statement (2.2): Noncompliance with CIP-006-6 R2.2 reduces the likelihood of an entity being able to properly investigate a cyber security event that occurs as a result of visitors to a PSP.

Risk Failure Statement (2.3): Noncompliance with CIP-006-6 R2.3 reduces the likelihood of an entity being able to properly investigate a cyber security event that occurs as a result of visitors to a PSP.

Risk Criteria

- What other sorts of physical protections were in place?
 - Video Surveillance



NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

- Guards
- Manned Facility
- What other sorts of electronic protections were in place?
 - Was there security monitoring of Cyber Assets?
 - Did assets require 2-Factor Authentication?
- Were visitors logged along with appropriate details?
- How long was the duration of the unescorted access?
 - How many individuals had unescorted access?
 - What did they have access to?
 - Sensitive areas increases risk.
 - Communal areas lowers risk.
- Were the unescorted visitors otherwise known or trusted?
 - Did they have active CIP Training, current Personnel Risk Assessments (PRAs) or otherwise trusted employee?
 - Did they have electronic access or other credentials needed to access Cyber Assets?
 - Were the unescorted visitors expected to arrive during the timeframe?
- What was the BES Impact Categorization?
- Was the noncompliant individual(s) responding to a CIP Exceptional Circumstance?
- Address actual harm

R2 Mitigation Verification

- For Verification Check
 - Are there process documents that discuss requirements to provide continuous escort?
 - Are there emails referring to providing continuous escort?
 - Are there videos showing continuous escort?
 - Has the entity provided digital logs or sign in sheets for entry into the PSP?
 - Are the digital logs complete? Do they show 90 days?



R3 Scoping and Risk Determination

R3. Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing program(s) that collectively include each of the applicable requirement parts in CIP-006-6 Table R3 – Maintenance and Testing Program.

3.1. Maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly.

R3 Scope Evaluation

- How many PACS or other locally mounted hardware or devices are in scope?

Noncompliant with R3.1	Entity failed to complete maintenance and testing of each PACS and locally mounted hardware or devices at the PSP at least once every 24 months.
------------------------	--

R3.1 Risk Determination

Risk Failure Statement: Noncompliance with CIP-006-6 R3.1 increases the likelihood that an entity would be unaware of door malfunctions or misuse of PACS potentially allowing unauthorized access within a PSP.

Risk Criteria

- Were the PACS otherwise functioning properly?
 - Were there any malfunctions detected?
 - Were PACS configured to alert for device errors?
- Were there other physical protections in place?
 - Guards
 - Video Surveillance
 - Manned Facilities
- Were there other electronic protections that protected assets beyond the PACS?
 - Were cyber assets capable of logging?
 - Were passwords changed from their defaults?
 - Were there any other electronic security monitoring in place?
- Establish the duration of the noncompliance
- Address actual harm

Tier 3: Major BES Disturbances	Caused or contributed to a major BES disturbance
Tier 2: Moderate Impact	IROL exceeded, BES limit (non-IROL SOL, frequency, voltage, or ACE) exceeded for >30 minutes, BES Facilities tripped unexpectedly, emergency action taken (e.g., reconfiguration, load



NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

	shed) to mitigate or prevent the impact of the violation, equipment damage, major (>50%) loss of visibility, control, state estimation, or contingency analysis for over 30 minutes
Tier 1: Minor Impact	Observations similar to those in tier 2 but of lesser magnitude, or loss of ability to monitor cybersecurity intrusions.
Tier 0: No Impact	No observed impact.

NPCC Specific Details

- XXX

Enforcement Notes

- XXXXX
- XXXX



CIP-007-6 Enforcement Approach

Background Information

- [CIP-007-6 Standard Language](#)
- [CIP-007-6 Implementation Plan](#)

Standard/Implementation Plan Effective Dates

- **United States**

Standard	Requirement	Effective Date
CIP-007-6	R1., R2., R3., R4., R5.	07/01/2016

Key Terminology

High Impact BES Cyber Systems

Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.

Medium Impact BES Cyber Systems

Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.

Medium Impact BES Cyber Systems without External Routable Connectivity

Only applies to medium impact BES Cyber Systems without External Routable Connectivity.

Medium Impact BES Cyber Systems with External Routable Connectivity

Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.

Electronic Access Control or Monitoring Systems (EACMS)

Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.



NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

Physical Access Control Systems (PACS)

Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

Protected Cyber Assets (PCA)

Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

Cyber Vulnerabilities and Exposures (CVE)

CVE IDs are a way to reference publicly-known information security vulnerabilities and exposures that are tracked by the National Vulnerabilities Database.



R1 Scoping and Risk Determination

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R1 – Ports and Services.

1.1. Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.

1.2. Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.

R1 Scope Evaluation

- How many ports that were not needed were enabled?
- How many physical input/output ports were left unprotected?
- Who would have had physical access to unprotected physical ports?
- What sort of rules prevented physical access to unprotected ports?
- What device or types of devices had ports unprotected?

- Specify which part was noncompliant

Noncompliant with R1.1	Entity failed to enable only needed logical network accessible ports.
Noncompliant with R1.2	Entity failed to protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.

R1. Risk Determination

Risk Failure Statement: Noncompliance with CIP-007-6 R1 increases the likelihood of a malicious actor exploiting an unnecessarily open port to gain electronic access to assets within the ESP.

Risk Criteria

- Identify the other physical protections of the assets or facility:
 - PSP – Do the assets reside within a PSP?
 - ESP – Are the assets within an ESP?
 - Were open ports only for authorized services?
 - Was this primarily a failure to document the justification for an open port?
 - How many assets were involved?
 - Can the assets be accessed remotely or does a user need to be physically present?



NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

- How many ports were left open or unjustified?
- Were the open ports accessible blocked elsewhere by firewalls?
- Were there other logical protections in place?
 - Whitelisting
 - Limited Privileges
 - Password Protection
 - Malicious code protection
 - Multi-Factor Authentication
- Address actual harm

R1 Mitigation Verification

- For Verification Check
 - Can the Entity provide work orders or change management documents showing the change or disabling of physical ports?
 - Can the Entity provide pictures of physical port protections?



R2 Scoping and Risk Determination

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R2 – Security Patch Management.

2.1. A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.

2.2. At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.

2.3. For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions:

- Apply the applicable patches; or
- Create a dated mitigation plan; or
- Revise an existing mitigation plan.

Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.

2.4. For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.

R2 Scope Evaluation

- How many patches were missed?
- How long beyond the 35-day window were patches not evaluated?
- How many devices were affected?

Noncompliant with R2.1	Entity failed to have a patch management process for tracking, evaluating, and installing cyber security patches.
Noncompliant with R2.2	Entity failed to evaluate security patches for applicability that have been released within 35 calendar days since the last evaluation from the source identified in R2.1
Noncompliant with R2.3	Entity failed to either apply patches, create a dated mitigation plan, or revise a mitigation plan within 35 days of the evaluation completion.



Noncompliant with R2.4	Entity failed to implement their dated mitigation plan created or revised in R2.3.
------------------------	--

R2 Risk Determination

Risk Failure Statement: Noncompliance with CIP-007-6 R2 reduces the Entity's ability to successfully monitor and address security updates in a timely manner. This failure may lead to an entity being unaware or leaving known security vulnerabilities unprotected or allowing a malicious actor to gain control of or render a BES Cyber System inoperable.

Risk Criteria

- Identify the other physical and logical protections of the assets or facility:
 - PSP – Do the assets reside within a PSP?
 - ESP – Do the assets within an ESP?
 - How many assets or devices were involved?
 - Can the assets be accessed remotely or does a user need to be physically present?
 - Did remote access require Multi-Factor Authentication?
 - How many patches were involved?
 - Were the patches critical?
 - Was the vulnerability the patch was intended to resolve difficult to exploit?
 - Were there other logical protections in place?
 - Intrusion Detection System (IDS)
 - Vulnerability Scanning
 - Antivirus Software
 - Baseline Configuration Monitoring
 - Security Event Monitoring
 - Were the assets in scope part of a segmented or isolated network?
- Address actual harm

R2 Mitigation Verification

- For Verification Check
 - Is there evidence of the patch being applied to the applicable devices?
 - Can the entity provide the dated mitigation plan?
 - Are there change management or work order documents showing the patches were applied?
 - Do the documents reference the correct CVE (Cyber Vulnerabilities and Exposures) ID number?



R3 Scoping and Risk Determination

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R3 – Malicious Code Prevention.

3.1. Deploy method(s) to deter, detect, or prevent malicious code.

3.2. Mitigate the threat of detected malicious code.

3.3. For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.

R3 Scope Evaluation

- How many devices were affected?

Noncompliant with R3.1	Entity failed to deploy methods to deter, detect, or prevent malicious code.
Noncompliant with R3.2	Entity failed to mitigate the threat of detected malicious code.
Noncompliant with R3.3	Entity failed to have a process for testing signatures or patterns used to deter, detect, or prevent malicious code.

R3 Risk Determination

Risk Failure Statement: Noncompliance with CIP-007-6 R3. increases the likelihood of malicious code executing and compromising the availability or integrity of a BES Cyber System.

Risk Criteria

- Identify the other physical and logical protections of the assets or facility:
 - PSP – Do the assets reside within a PSP?
 - Was physical access and/or logical access restricted?
 - ESP – Do the assets reside within an ESP?
 - How many assets or devices were involved?
 - Can the assets be accessed remotely or does a user need to be physically present?
 - Did remote access require Multi-Factor Authentication?
 - Were there other means used to prevent malicious code?
 - Were other credentials needed to access the devices in scope?
 - Was there other monitoring?
 - Were there other supporting protections?
 - Intrusion Detection Systems/Intrusion Prevention Systems (layers of IDS)



NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

- Security Event Monitoring systems/Security Incident and Event Management (SIEM) systems?
- Did network architecture reduce the risk?
 - Were there firewalls in place providing supportive protection?
 - Host-based firewalls (Directly on asset)
 - Layers of firewalls controlling traffic
 - Intermediate System in place
 - Was there a separated, segmented, or isolated network?
- What was the BES Impact Categorization?
- Address actual harm

R3 Mitigation Verification

- For Verification Check
 - Is there evidence of the testing of signatures or patterns?
 - Is there evidence from the antivirus or malicious code prevention provider?
 - Is there evidence of malicious code prevention currently in place?

Tier 3: Major BES Disturbances	Caused or contributed to a major BES disturbance
Tier 2: Moderate Impact	IROL exceeded, BES limit (non-IROL SOL, frequency, voltage, or ACE) exceeded for >30 minutes, BES Facilities tripped unexpectedly, emergency action taken (e.g., reconfiguration, load shed) to mitigate or prevent the impact of the violation, equipment damage, major (>50%) loss of visibility, control, state estimation, or contingency analysis for over 30 minutes
Tier 1: Minor Impact	Observations similar to those in tier 2 but of lesser magnitude, or loss of ability to monitor cybersecurity intrusions.
Tier 0: No Impact	No observed impact.



R4 Scoping and Risk Determination

R4. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R4 – Security Event Monitoring.

4.1. Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events:

4.1.1. Detected successful login attempts;

4.1.2. Detected failed access attempts and failed login attempts;

4.1.3. Detected malicious code.

4.2. Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability):

4.2.1. Detected malicious code from Part 4.1; and

4.2.2. Detected failure of Part 4.1 event logging.

4.3. Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances.

4.4. Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.

R4 Scope Evaluation

- How long were events not being logged or did not have alerting?
- How many assets were not being logged or did not have alerting?
- How long were logs stored if not 90 days?
- How long was it between reviews of logged events?
- Specify which part was noncompliant

Noncompliant with R4.1	Entity failed to log events at the BES Cyber System level or Cyber Asset level for Cyber Security Incidents.
Noncompliant with R4.1.1	Entity failed to log events for detected successful login attempts.
Noncompliant with R4.1.2	Entity failed to log events for detected failed access and login attempts.
Noncompliant with R4.1.3	Entity failed to log events for detected malicious code.



Noncompliant with R4.2	Entity failed to generate alerts for security events that the Entity determines necessitates an alert.
Noncompliant with R4.2.1	Entity failed to generate an alert for detected malicious code.
Noncompliant with R4.2.2	Entity failed to generate an alert for detected failure of R4.1. event logging.
Noncompliant with R4.3	Entity failed to retain event logs for 90 days.
See Notes	
Noncompliant with R4.4	Entity failed to review a summarization or sampling of logged events within 15 days to identify undetected Cyber Security Incidents.

R4 Risk Determination

Risk Failure Statement: Noncompliance with CIP-007-6 R4 decreases the likelihood of detecting a cyber security event through logs and hampers the ability to investigate any incident afterwards.

Risk Criteria

- Identify the other physical and logical protections of the assets or facility:
 - PSP – Do the assets reside within a PSP?
 - Was physical access and/or logical access restricted?
 - ESP – Do the assets reside within an ESP?
 - How many assets or devices were involved?
 - Can the assets be accessed remotely or does a user need to be physically present?
 - Did remote access require Multi-Factor Authentication?
 - Were there other means used to prevent malicious code?
 - Were other credentials needed to access the devices in scope?
 - Was there other monitoring?
 - Were the devices firmware-based?
 - Were there other supporting protections?
 - Were Firewall logs being captured?
 - Were Intrusion Detection Systems/Intrusion Prevention Systems (layers of IDS) used for reviewing network traffic?
 - Was antivirus or some type of malicious communication detection deployed?
 - Security Event Monitoring systems/Security Incident and Event Management (SIEM) systems?
- Were there procedural protections?
 - Were there daily or weekly reviews of logs?



NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

- Were there partial log reviews?
- Were there other types of logging still being completed?
- Did network architecture reduce the risk?
 - Were there firewalls in place providing supportive protection?
 - Layers of firewalls controlling traffic
 - Intermediate System in place
- What was the BES Impact Categorization?
- Address actual harm

R4 Mitigation Verification

- For Verification Check
 - Can the Entity provide examples of logging that has been accomplished?
 - Can the Entity provide screenshots of dashboards and other tools used for monitoring logging or alerting?
 - Can the Entity provide process documents outlining processes showing reviews are conducted regularly for cyber security incidents?
 - Can the Entity provide reports or screenshots from Intrusion Detection Systems?
 - Are there any other documentary trails of evidence for log reviews that can be provided?

Tier 3: Major BES Disturbances	Caused or contributed to a major BES disturbance
Tier 2: Moderate Impact	IROL exceeded, BES limit (non-IROL SOL, frequency, voltage, or ACE) exceeded for >30 minutes, BES Facilities tripped unexpectedly, emergency action taken (e.g., reconfiguration, load shed) to mitigate or prevent the impact of the violation, equipment damage, major (>50%) loss of visibility, control, state estimation, or contingency analysis for over 30 minutes
Tier 1: Minor Impact	Observations similar to those in tier 2 but of lesser magnitude, or loss of ability to monitor cybersecurity intrusions.
Tier 0: No Impact	No observed impact.

R5 Scoping and Risk Determination

R5. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R5 – System Access Controls.



- 5.1.** Have a method(s) to enforce authentication of interactive user access, where technically feasible.
- 5.2.** Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).
- 5.3.** Identify individuals who have authorized access to shared accounts.
- 5.4.** Change known default passwords, per Cyber Asset capability.
- 5.5.** For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters:
 - 5.5.1.** Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and
 - 5.5.2.** Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.
- 5.6.** Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.
- 5.7.** Where technically feasible, either:
 - Limit the number of unsuccessful authentication attempts; or
 - Generate alerts after a threshold of unsuccessful authentication attempts.

R5 Scope Evaluation

- How many devices failed to enforce authentication?
- How many default or generic account types were missed being identified and inventoried?
- How many individuals were identified as having access to shared accounts?
- How many devices did not enforce password length or complexity requirements?
- How many individuals had access to the devices in scope?
- How long has it been since passwords were last changed?
- How many devices did not limit or provide alerts based on unsuccessful authentication attempts?

Noncompliant with R5.1	Entity failed to have a method to enforce authentication of interactive user access.
Noncompliant with R5.2	Entity failed to identify and inventory all known enabled default or other generic account types.
Noncompliant with R5.3	Entity failed to identify individuals who have authorized access to shared accounts.



Noncompliant with R5.4	Entity failed to change known default passwords.
Noncompliant with R5.5	Entity failed to technically or procedurally enforce password parameters for password-only authentication for interactive user access.
Noncompliant with R5.5.1	Entity failed to enforce password length requirements.
Noncompliant with R5.5.2	Entity failed to enforce password complexity requirements.
Noncompliant with R5.6	Entity failed to change passwords every 15 months.
Noncompliant with R5.7	Entity failed to limit the number of unsuccessful authentication attempts or generate alerts after a threshold of attempts has been met.

R5 Risk Determination

Risk Failure Statement: Noncompliance with CIP-007-6 R5 increases the likelihood of an unauthorized individual gaining electronic access.

Risk Criteria

- Identify the other physical and logical protections of the assets or facility:
 - PSP – Do the assets reside within a PSP?
 - Was physical access and/or logical access restricted?
 - Were those with access trusted? (CIP Training, PRA, or other)
 - Was there logging of physical access?
 - ESP – Do the assets reside within an ESP?
 - How many assets or devices were involved?
 - Can the assets be accessed remotely or does a user need to be physically present?
 - Did remote access require Multi-Factor Authentication?
 - Were other credentials needed to access the devices in scope?
 - Was there other types of monitoring or alerting?
 - Were the devices firmware-based?
 - Were there other supporting protections?
 - Were Firewall logs being captured?
 - Were default passwords changed?
 - Did passwords meet length and complexity requirements?
 - Were Intrusion Detection Systems/Intrusion Prevention Systems (layers of IDS) used for reviewing network traffic?
 - Was antivirus or some type of malicious communication detection deployed?



NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

- Security Event Monitoring systems/Security Incident and Event Management (SIEM) systems? (or a Security Operations Center?)
- Were accounts in scope interactive or shared user accounts?
- Did network architecture reduce the risk?
 - Were there firewalls in place providing supportive protection?
 - Layers of firewalls controlling traffic
 - Was an Intermediate System in place?
- What was the BES Impact Categorization?
- Address actual harm

R5 Mitigation Verification

- For Verification Check
 - Can the Entity provide an inventory of enabled account types?
 - Is the Entity able to provide a list of individuals authorized with access to shared accounts?
 - Are there change management or work order documents showing passwords were changed?
 - Can the Entity provide checklists or spreadsheets that shows passwords meet length and complexity requirements?
 - How many devices were affected?
 - Can the Entity show evidence of limits on unsuccessful login attempts?
 - Can the Entity provide screenshots of alerts after a threshold of failed login attempts?

Tier 3: Major BES Disturbances	Caused or contributed to a major BES disturbance
Tier 2: Moderate Impact	IROL exceeded, BES limit (non-IROL SOL, frequency, voltage, or ACE) exceeded for >30 minutes, BES Facilities tripped unexpectedly, emergency action taken (e.g., reconfiguration, load shed) to mitigate or prevent the impact of the violation, equipment damage, major (>50%) loss of visibility, control, state estimation, or contingency analysis for over 30 minutes
Tier 1: Minor Impact	Observations similar to those in tier 2 but of lesser magnitude, or loss of ability to monitor cybersecurity intrusions.
Tier 0: No Impact	No observed impact.



NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

NPCC Specific Details

- XXX

Enforcement Notes

- CIP-007-6 R4.3
 - CCTF Discussion Topic: [CIP-007-6 R4.3 TFE's for devices that are not capable of logging - Flat \(nerc.net\)](#)
 - "If an entity can show that a BCA, EACMS, PACS, or PCA is not capable of logging under CIP-007-6 R4 Part 4.1 then there is no reason to file a TFE under Part 4.3 since there were no logs identified in Part 4.1. Requiring a TFE has no impact on the risk or reliability of the BES and becomes nothing more than unnecessary overhead for the entity and the regional authority."



FAC-008-5 Enforcement Approach

Background Information

- [FAC-008-5 Standard Language](#)

Standard Effective Dates and Applicable Functions

- United States

Standard	Requirement	Effective Date	Applicable Function
FAC-008-5	R1., R2.	10/1/2021	Generator Owner (GO)
FAC-008-5	R3.	10/1/2021	Transmission Owner (TO)
FAC-008-5	R4., R5.	Retired on 1/21/2014	N/A
FAC-008-5	R6.	10/1/2021	Generator Owner (GO) and Transmission Owner (TO)
FAC-008-5	R7.	Retired 10/1/2021	N/A
FAC-008-5	R8.	10/1/2021	Transmission Owner (TO) and Generator Owner (GO)*

- Quebec

Standard	Requirement	Effective Date	Applicable Function
FAC-008-5	R1., R2.	4/1/2022	Generator Owner (GO)
FAC-008-5	R3.	4/1/2022	Transmission Owner (TO)
FAC-008-5	R4., R5.	??	N/A
FAC-008-5	R6.	4/1/2022	Generator Owner (GO) and Transmission Owner (TO)
FAC-008-5	R7.	??	N/A
FAC-008-5	R8.	4/1/2022	Transmission Owner (TO) and Generator Owner (GO)*

Key Terminology

Applicable Facilities:

- All electrical Facilities (generators, transmission elements such as feeders and transformers, etc.) and respective component equipment (breakers, disconnect switches, etc.) that are required for the reliable planning and operation of the Bulk Electric System (BES). Generating plant/Facility greater than 75 MVA (gross aggregate nameplate rating) directly connected to the Bulk Electric System.

Facility



NORTHEAST POWER COORDINATING COUNCIL, INC.

A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)



R1 Scoping and Risk Determination

R1. Each GO shall have documentation for determining the Facility Ratings of its solely and jointly owned generator Facility(ies) up to the low side terminals of the main step up transformer if the GO does not own the main step up transformer and the high side terminals of the main step up transformer if the GO owns the main step up transformer. [Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]

- 1.1. The documentation shall contain assumptions used to rate the generator and at least one of the following:
 - Design or construction information such as design criteria, ratings provided by equipment manufacturers, equipment drawings and/or specifications, engineering analyses, method(s) consistent with industry standards (e.g. ANSI and IEEE), or an established engineering practice that has been verified by testing or engineering analysis.
 - Operational information such as commissioning test results, performance testing or historical performance records, any of which may be supplemented by engineering analyses.
- 1.2. The documentation shall be consistent with the principle that the Facility Ratings do not exceed the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility.

R1 Scope Evaluation

- Establish the number of applicable generating Facilities

Noncompliant with R1	Entity failed to have documentation for determining the Facility Ratings of its solely and jointly owned generator Facility(ies) up to the low side terminals of the main generator step-up (GSU) transformer if the GO does not own the main GSU transformer and the high side terminals of the main GSU transformer if the GO owns the main GSU transformer.
Noncompliant with R1, Part 1.1	Entity's documentation failed to contain assumptions used to rate the generator(s) and at least one of the following: <ul style="list-style-type: none">• Design criteria, ratings provided by equipment manufacturers, equipment drawings and/or specifications, engineering analyses, method(s) consistent with industry standards (e.g. ANSI and IEEE), or an established engineering practice that has been verified by testing or engineering analysis.• Operational information such as commissioning test results, performance testing or historical performance records, any of which may be supplemented by engineering analyses.
Noncompliant with R1, Part 1.2	Entity's documentation failed to be consistent with the principle that the Facility Ratings do not exceed the most limiting applicable Equipment (MLE) Rating of the individual equipment that comprises that Facility.



R1 Risk Determination

Risk Failure Statement: Noncompliance with FAC-008-5 R1 may result in Facility Ratings that are inconsistent with industry standards. This may result in generating Facilities being operated in excess of their correct thermal capacity, cause equipment damage, or lead to an incorrect determination of System Operating Limits.

Risk Criteria

- Identify the inherent properties of the Entity's noncompliant BES Facility(ies).
 - Generating Facility
 - Total output (MW)
 - Capacity Factor during the duration of the noncompliance
 - Classification as a critical resource or black-start unit
 - Variable resources (wind, solar, hydro)
 - Transmission Facility (if applicable)
 - Total customer load served/lost
 - Operating voltage (kV)
 - Part of IROLs or Inter-Area and Intra-Area interface(s)
 - Entity's Reliability Coordinator's required operating reserve
- Identify compensating controls/aggravating factors:
 - Does the entity monitor their equipment in real time?
 - Address the entity's facility's historical operation
 - Did the entity perform other Reliability assessments or Capacity tests?
 - Did the Reliability Coordinator or Transmission Operator have situation awareness of the most limiting element or the change in Facility Rating?
- Quality of internal compliance controls/procedures
 - Was the noncompliance self-identified
- Impact on Facility ratings
 - How many applicable BES Facilities were affected by the noncompliance?
 - Identify the extent of adjustment.
- Address duration
- Address actual harm.

Tier 3: Major BES Disturbances	Caused or contributed to a major BES disturbance
Tier 2: Moderate Impact	IROL exceeded, BES limit (non-IROL SOL, frequency, voltage, or ACE) exceeded for >30 minutes, BES Facilities tripped unexpectedly, emergency action taken (e.g., reconfiguration, load shed) to mitigate or prevent the impact of the violation, equipment damage, major (>50%) loss of visibility, control, state estimation, or contingency analysis for over 30 minutes
Tier 1: Minor Impact	Observations similar to those in tier 2 but of lesser magnitude, or loss of ability to monitor cybersecurity intrusions.



Tier 0: No Impact	No observed impact.

R1 Mitigation Verification

- For each generating Facility, request electronic copies of Demarcation Diagrams (aka One-line Diagrams) as evidence of equipment owned by the Entity up to the Point of Interconnection (POI) to the host Transmission Owner (TO).
 - o For each generating Facility, identify the main GSU and its operating characteristics (low side voltage and high side voltage). Establish ownership of the main GSU.
 - If the Entity does not own the main GSU, then the Entity's POI to its host TO is the low side of the GSU, and the Entity is required to only comply with R1 and not R2.
 - If the Entity owns the GSU, then request the Entity to identify its POI with the host TO.
 - If the POI is other than the high side of the main GSU, then the Entity is required to comply with R2 as well as R1.
- Does the Entity possess a proprietary FRM document, dated and signed, for Facility Ratings of its applicable Facilities that spans the entirety of the standard/requirement effective period?
 - o Is the FRM consistent with the principle that the Facility Ratings do not exceed the MLE Rating of the individual equipment that comprises that Facility?
 - o Does the FRM provide for calculations of ratings in MVA or Amps at nominal operating voltages?
 - o Does the document include assumptions and methods used to determine Normal and Emergency Facility Ratings, as applicable?
 - o Ratings for Summer and Winter operating periods required at a minimum
 - o Basis for individual ratings and permitted duration of operation
 - o Ensure that re-ratings of any existing equipment (including generator) has been reflected in the most current FRM document.
- Determine the Entity's Extent of Condition (EOC) by ensuring that the Entity has had an appropriate FRM document for earlier versions of the standard.
 - o Verify compliance starting from June 18, 2007, the date when Standard FAC-008-1 (R1) became effective.
- Determine the duration of the noncompliance based on whether an FRM document actually existed when required, or whether an existing FRM failed to include assumptions regarding rated generator capacity, or failed to include individual pieces of equipment that comprise the Facility, or failed to ensure that the Facility Ratings do not exceed the most limiting applicable Equipment (MLE) rating, etc.
- Extent of Scope - If the Entity's FRM document is noncompliant, then an extent of scope must be conducted that includes, at a minimum, a potential noncompliance of requirement R6.



R2 Scoping and Risk Determination

R2. Each GO shall have a documented methodology for determining Facility Ratings (Facility Ratings methodology) of its solely and jointly owned equipment connected between the location specified in R1 and the point of interconnection with the TO that contains all of the following. [Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]

- 2.1. The methodology used to establish the Ratings of the equipment that comprises the Facility(ies) shall be consistent with at least one of the following:
 - Ratings provided by equipment manufacturers or obtained from equipment manufacturer specifications such as nameplate rating.
 - One or more industry standards developed through an open process such as Institute of Electrical and Electronic Engineers (IEEE) or International Council on Large Electric Systems (CIGRE).
 - A practice that has been verified by testing, performance history or engineering analysis.
- 2.2. The underlying assumptions, design criteria, and methods used to determine the Equipment Ratings identified in Requirement R2, Part 2.1 including identification of how each of the following were considered:
 - 2.2.1 Equipment Rating standard(s) used in development of this methodology.
 - 2.2.2 Ratings provided by equipment manufacturers or obtained from equipment manufacturer specifications.
 - 2.2.3 Ambient conditions (for particular or average conditions or as they vary in real-time).
 - 2.2.4 Operating limitations, such as temporary de-ratings of impaired equipment in accordance with good utility practice
- 2.3. A statement that a Facility Rating shall respect the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility.
- 2.4. The process by which the Rating of equipment that comprises a Facility is determined.
 - 2.4.1 The scope of equipment addressed shall include, but not be limited to, conductors, transformers, relay protective devices, terminal equipment, and series and shunt compensation devices.
 - 2.4.2 The scope of Ratings addressed shall include, as a minimum, both Normal and Emergency Ratings.

R2 Scope Evaluation

Noncompliant with R2	Entity failed to establish a documented Facility Ratings Methodology (FRM) for determining Facility Ratings of its solely and jointly owned equipment connected between the location specified in R1 and the
----------------------	--



	point of interconnection with the TO that contains all of the information required by Part 2.1 through Part 2.4
Noncompliant with R2, Part 2.1	Entity's FRM failed to be consistent with at least one of the following: <ul style="list-style-type: none">• Ratings provided by equipment manufacturers or from equipment manufacturer specifications such as nameplate rating.• One or more industry standards developed through an open process such as Institute of Electrical and Electronic Engineers (IEEE) or International Council on Large Electric Systems (CIGRE).• A practice that has been verified by testing, performance history or engineering analysis

Noncompliant with R2, Part 2.2	Entity's FRM documentation failed to include the underlying assumptions, design criteria, and methods used to determine the Equipment Ratings identified in R2, Part 2.1 including identification of how each of the factors in Parts 2.2.1 through 2.2.4 were considered
Noncompliant with R2, Part 2.2.1	Entity's FRM documentation failed to include consideration for Equipment Rating standard(s) used in development of this methodology.
Noncompliant with R2, Part 2.2.2	Entity's FRM documentation failed to include consideration for ratings provided by equipment manufacturers or obtained from equipment manufacturer specifications.
Noncompliant with R2, Part 2.2.3	Entity's FRM documentation failed to include consideration for ambient conditions (for particular or average conditions or as they vary in real-time).
Noncompliant with R2, Part 2.2.4	Entity's FRM documentation failed to include consideration for operating limitations, such as temporary de-ratings of impaired equipment in accordance with good utility practice.

Noncompliant with R2, Part 2.3	Entity's FRM documentation failed to contain a statement that a Facility Rating shall respect the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility.
--------------------------------	---

Noncompliant with R2, Part 2.4	Entity's FRM documentation failed to contain a process by which the Rating of equipment that comprises a Facility is determined.
Noncompliant with R2, Part 2.4.1	Entity's FRM documentation failed to identify the scope of equipment addressed, which shall include, but not be limited to, conductors, transformers, relay protective devices, terminal equipment, and series and shunt compensation devices.
Noncompliant with R2, Part 2.4.2	Entity's FRM documentation failed to identify the scope of ratings addressed, which shall include, as a minimum, both Normal and Emergency Ratings.

R2 Risk Determination

Risk Failure Statement: Noncompliance with FAC-008-5 R2 may result in Facility Ratings that are inconsistent with industry standards. This may result in



generating Facilities being operated in excess of their correct thermal capacity, cause equipment damage, or lead to an incorrect determination of System Operating Limits.

Risk Criteria

- Identify the inherent properties of the Entity's noncompliant BES Facility(ies).
 - Generating Facility
 - Total output (MW)
 - Capacity Factor during the duration of the noncompliance
 - Classification as a critical resource or black-start unit
 - Variable resources (wind, solar, hydro)
 - Transmission Facility (if applicable)
 - Total customer load served/lost
 - Operating voltage (kV)
 - Part of IROLs or Inter-Area and Intra-Area interface(s)
 - Entity's Reliability Coordinator's required operating reserve
- Identify compensating controls/aggravating factors:
 - Does the entity monitor their equipment in real time?
 - Address the facility(ies)'s historical operation
 - Did the entity perform other Reliability assessments or Capacity tests?
 - Did the Reliability Coordinator or Transmission Operator have situation awareness of the most limiting element or the change in Facility Rating?
- Quality of internal compliance controls/procedures
 - Was the noncompliance self-identified
- Impact on Facility ratings
 - How many applicable BES Facilities were affected by the noncompliance?
 - Identify the extent of adjustment.
- Address duration
- Address actual harm.

Tier 3: Major BES Disturbances	Caused or contributed to a major BES disturbance
Tier 2: Moderate Impact	IROL exceeded, BES limit (non-IROL SOL, frequency, voltage, or ACE) exceeded for >30 minutes, BES Facilities tripped unexpectedly, emergency action taken (e.g., reconfiguration, load shed) to mitigate or prevent the impact of the violation, equipment damage, major (>50%) loss of visibility, control, state estimation, or contingency analysis for over 30 minutes
Tier 1: Minor Impact	Observations similar to those in tier 2 but of lesser magnitude, or loss of ability to monitor cybersecurity intrusions.
Tier 0: No Impact	No observed impact.



R2 Mitigation Verification

- For each generating Facility, request electronic copies of Demarcation Diagrams (aka One-line Diagrams) as evidence of equipment owned by the Entity up to the Point of Interconnection (POI) to the host Transmission Owner (TO).
 - o For each generating Facility, identify the main GSU and its operating characteristics (low side voltage and high side voltage). Establish ownership of the main GSU.
 - If the Entity does not own the main GSU, then the Entity's POI to its host TO is the low side of the GSU, and the Entity is required to only comply with R1 and not R2.
 - If the Entity owns the GSU, then request the Entity to identify its POI with the host TO.
 - If the POI is other than the high side of the main GSU, then the Entity is required to comply with R2 as well as R1.
- Does the Entity possess a proprietary FRM document, dated and signed, for Facility Ratings of its applicable Facilities that spans the entirety of the standard/requirement effective period?
 - o Is the FRM consistent with the principle that the Facility Ratings do not exceed the MLE Rating of the individual equipment that comprises that Facility?
 - o Does the FRM provide for calculations of ratings in MVA or Amps at nominal operating voltages?
 - o Does the document include assumptions and methods used to determine Normal and Emergency Facility Ratings, as applicable?
 - o Ratings for Summer and Winter operating periods required at a minimum
 - o Basis for individual ratings and permitted duration of operation
 - o Ensure that re-ratings of any existing equipment (including generator) has been reflected in the most current FRM document.
- Determine the Entity's Extent of Condition (EOC) by ensuring that the Entity has had an appropriate FRM document for earlier versions of the standard.
 - o Verify compliance starting from June 18, 2007, the date when Standard FAC-008-1 (R1) became effective.
- Determine the duration of the noncompliance based on whether an FRM document actually existed when required, or whether an existing FRM failed to include assumptions regarding rated generator capacity, or failed to include individual pieces of equipment that comprise the Facility, or failed to ensure that the Facility Ratings do not exceed the most limiting applicable Equipment (MLE) rating, etc.
- Extent of Scope - If the Entity's FRM document is noncompliant, then an extent of scope must be conducted that includes, at a minimum, a potential noncompliance of requirement R6.



R3 Scoping and Risk Determination

R3. Each TO shall have a documented methodology for determining Facility Ratings (Facility Ratings methodology) of its solely and jointly owned Facilities (except for those generating unit Facilities addressed in R1 and R2) that contains all of the following:
[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]

- 3.1** The methodology used to establish the Ratings of the equipment that comprises the Facility(ies) shall be consistent with at least one of the following:
- Ratings provided by equipment manufacturers or obtained from equipment manufacturer specifications such as nameplate rating.
 - One or more industry standards developed through an open process such as Institute of Electrical and Electronic Engineers (IEEE) or International Council on Large Electric Systems (CIGRE).
 - A practice that has been verified by testing, performance history or engineering analysis.
- 3.2** The underlying assumptions, design criteria, and methods used to determine the Equipment Ratings identified in Requirement R2, Part 2.1 including identification of how each of the following were considered:
- 3.2.1** Equipment Rating standard(s) used in development of this methodology.
- 3.2.2** Ratings provided by equipment manufacturers or obtained from equipment manufacturer specifications.
- 3.2.3** Ambient conditions (for particular or average conditions or as they vary in real-time).
- 3.2.4** Operating limitations, such as temporary de-ratings of impaired equipment in accordance with good utility practice
- 3.3** A statement that a Facility Rating shall respect the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility.
- 3.4** The process by which the Rating of equipment that comprises a Facility is determined.
- 3.4.1** The scope of equipment addressed shall include, but not be limited to, conductors, transformers, relay protective devices, terminal equipment, and series and shunt compensation devices.
- 3.4.2** The scope of Ratings addressed shall include, as a minimum, both Normal and Emergency Ratings.

R3 Scope Evaluation

Noncompliant with R3	Entity failed to establish a documented Facility Ratings Methodology (FRM) for determining Facility Ratings of its solely and jointly owned Facilities (except for those generating unit Facilities addressed in R1 and R2) that contains all of the information required by Part 3.1. through Part 3.4.
Noncompliant with R3, Part 3.1	Entity's FRM failed to be consistent with at least one of the following: <ul style="list-style-type: none">• Ratings provided by equipment manufacturers or from equipment manufacturer specifications such as nameplate rating.• One or more industry standards developed through an open process such as Institute of Electrical and Electronic Engineers (IEEE) or International Council on Large Electric Systems (CIGRE).



	<ul style="list-style-type: none"> A practice that has been verified by testing, performance history or engineering analysis.
Noncompliant with R3, Part 3.2	Entity's FRM documentation failed to include the underlying assumptions, design criteria, and methods used to determine the Equipment Ratings identified in R3, Part 3.1 including identification of how each of the factors discussed in Parts 3.2.1 through 3.2.4 were considered.
Noncompliant with R3, Part 3.2.1	Entity's FRM documentation failed to include consideration for Equipment Rating standard(s) used in development of this methodology.
Noncompliant with R3, Part 3.2.2	Entity's FRM documentation failed to include consideration for ratings provided by equipment manufacturers or obtained from equipment manufacturer specifications.
Noncompliant with R3, Part 3.2.3	Entity's FRM documentation failed to include consideration for ambient conditions (for particular or average conditions or as they vary in real-time).
Noncompliant with R3, Part 3.2.4	Entity's FRM documentation failed to include consideration for operating limitations, such as temporary de-ratings of impaired equipment in accordance with good utility practice.
Noncompliant with R3, Part 3.3	Entity's FRM documentation failed to contain a statement that a Facility Rating shall respect the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility.
Noncompliant with R3, Part 3.4	Entity's FRM documentation failed to contain a process by which the Rating of equipment that comprises a Facility is determined.
Noncompliant with R3, Part 3.4.1	Entity's FRM documentation failed to identify the scope of equipment addressed, which shall include, but not be limited to, conductors, transformers, relay protective devices, terminal equipment, and series and shunt compensation devices.
Noncompliant with R3, Part 3.4.2	Entity's FRM documentation failed to identify the scope of ratings addressed, which shall include, as a minimum, both Normal and Emergency Ratings.

Risk Determination

Risk Failure Statement: Noncompliance with MOD-025-2 R3 reduces the accuracy of the Transmission Planner's models and planning studies used to assess system reliability.

Risk Criteria

- Identify the inherent properties of the Entity's noncompliant BES Facility(ies).
 - Transmission Facility
 - Total customer load served/lost
 - Operating voltage (kV)
 - Part of IROLs or Inter-Area and Intra-Area interface(s)
 - Entity's Reliability Coordinator's required operating reserve
- Identify compensating controls/aggravating factors:
 - Does the entity monitor their equipment in real time?
 - Address the facility(ies)'s historical operation
 - Did the entity perform other Reliability assessments or Capacity tests?



- Did the Reliability Coordinator or Transmission Operator have situation awareness of the most limiting element or the change in Facility Rating?
- Quality of internal compliance controls/procedures
 - Was the noncompliance self-identified
- Impact on Facility ratings
 - How many applicable BES Facilities were affected by the noncompliance?
 - Identify the extent of adjustment.
- Address duration
- Address actual harm.

Tier 3: Major BES Disturbances	Caused or contributed to a major BES disturbance
Tier 2: Moderate Impact	IROL exceeded, BES limit (non-IROL SOL, frequency, voltage, or ACE) exceeded for >30 minutes, BES Facilities tripped unexpectedly, emergency action taken (e.g., reconfiguration, load shed) to mitigate or prevent the impact of the violation, equipment damage, major (>50%) loss of visibility, control, state estimation, or contingency analysis for over 30 minutes
Tier 1: Minor Impact	Observations similar to those in tier 2 but of lesser magnitude, or loss of ability to monitor cybersecurity intrusions.
Tier 0: No Impact	No observed impact.

R3 Mitigation Verification

- Establish the number of transmission/generating Facilities applicable to the standard. Depending on the extent of the noncompliance and/or complexity of the case, request a breakdown of the Entity's Facilities by:
 - Substations
 - Transmission feeders
 - Shunt/Series Capacitors
 - Shunt/Series Reactors
 - SVCs
 - Transformers
 - Generators
 - Others (bus ties, T-taps, etc.)
- As applicable to the specific case, request electronic copies of Demarcation Diagrams (aka One-line Diagrams) as evidence of equipment owned by the Entity up to the Point of Interconnection (POI) with interconnecting TOs and GOs.
- Does the Entity possess a proprietary FRM document, dated and signed, for Facility Ratings of its applicable Facilities that spans the entirety of the standard/requirement effective period?
 - Is the FRM consistent with the principle that the Facility Ratings do not exceed the MLE Rating of the individual equipment that comprises that Facility?
 - Does the FRM provide for calculation of ratings in MVA/Amps at nominal operating voltages?



- Does the document include assumptions and methods used to determine Normal and Emergency Facility Ratings, as applicable?
 - Ratings for Summer and Winter operating periods required at a minimum
 - Basis for individual ratings and permitted duration of operation
 - Ensure that re-ratings of and modifications to any existing equipment have been reflected in the FRM document.
- Determine the Entity's Extent of Condition (EOC) by ensuring that the Entity has had an appropriate FRM document for earlier versions of the standard.
 - Verify compliance starting from June 18, 2007, the date when Standard FAC-008-1 (R1) became effective.
- Determine the duration of the noncompliance based on missed FRM documentation or the existing FRM's failure to include assumptions for rating equipment thermal capacity, failure to include individual pieces of equipment that comprise the Facility, failure to ensure that the Facility Ratings do not exceed the most limiting applicable Equipment (MLE) rating, etc.
- Extent of Scope - If the Entity's FRM document is noncompliant, then an extent of scope must be conducted that includes, at a minimum, a potential noncompliance of requirement R6.



R6 Scoping and Risk Determination

R6. Each TO and GO shall have Facility Ratings for its solely and jointly owned Facilities that are consistent with the associated Facility Ratings methodology or documentation for determining its Facility Ratings. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]

R6 Scope Evaluation

- Establish the number of applicable generating Facilities

Noncompliant with R6	The Entity failed to determine Facility Ratings consistent with the associated Facility Ratings methodology (FRM) or documentation for determining its Facility Ratings.
----------------------	--

R6 Risk Determination

Risk Failure Statement: Noncompliance of FAC-008-5 R6 increases the potential for its Facilities to be operated in excess of their correct capacity rating, creating the opportunity for equipment damage, and incorrect determination of System Operating Limits for use in system planning and real-time operation.

Risk Criteria

- Identify the inherent properties of the Entity's noncompliant BES Facility(ies).
 - Generating Facility
 - Total output (MW)
 - Capacity Factor during the duration of the noncompliance
 - Classification as a critical resource or black-start unit
 - Variable resources (wind, solar, hydro)
 - Transmission Facility (if applicable)
 - Total customer load served/lost
 - Operating voltage (kV)
 - Part of IROLs or Inter-Area and Intra-Area interface(s)
 - Entity's Reliability Coordinator's required operating reserve
- Identify compensating controls/aggravating factors:
 - Does the entity monitor their equipment in real time?
 - Address the facility(ies)'s historical operation
 - Did the entity perform other Reliability assessments or Capacity tests?
 - Did the Reliability Coordinator or Transmission Operator have situation awareness of the most limiting element or the change in Facility Rating?
- Quality of internal compliance controls/procedures
 - Was the noncompliance self-identified
- Impact on Facility ratings
 - How many applicable BES Facilities were affected by the noncompliance?
 - Identify the number of Facilities requiring derates
 - Identify the extent of adjustment.
 - Identify if the component(s) at issue are the most limiting element (MLE) of the Facility
- Address duration



- Address actual harm.

Tier 3: Major BES Disturbances	Caused or contributed to a major BES disturbance
Tier 2: Moderate Impact	IROL exceeded, BES limit (non-IROL SOL, frequency, voltage, or ACE) exceeded for >30 minutes, BES Facilities tripped unexpectedly, emergency action taken (e.g., reconfiguration, load shed) to mitigate or prevent the impact of the violation, equipment damage, major (>50%) loss of visibility, control, state estimation, or contingency analysis for over 30 minutes
Tier 1: Minor Impact	Observations similar to those in tier 2 but of lesser magnitude, or loss of ability to monitor cybersecurity intrusions.
Tier 0: No Impact	No observed impact.

R6 Mitigation Verification and Other Considerations

- Establish the number of transmission/generating Facilities applicable to the standard. Depending on the extent of the noncompliance and/or complexity of the case, request a breakdown of the Entity's Facilities by:
 - Substations
 - Generating Facilities
 - Transmission feeders
 - Shunt/Series Capacitors
 - Shunt/Series Reactors
 - SVCs
 - Transformers
 - Generators
 - Others (bus ties, T-taps, etc.)
- As applicable to the specific case, request electronic copies of Demarcation Diagrams (aka One-line Diagrams) as evidence of equipment owned by the Entity up to the Point of Interconnection (POI) with interconnecting TOs and GOs.
- Does the Entity possess a proprietary FRM document, dated and signed, for Facility Ratings of its applicable Facilities that spans the entirety of the standard/requirement effective period (required by FERC/NERC)?
 - Did the Entity consider "Actual Field conditions" in its determination of Facility Ratings (i.e.: field inspections)?
 - Clearance/sagging issues, deteriorated condition of equipment, etc.
 - Does the Entity's provide Facility ratings in MVA/Amps at nominal operating voltages?
 - Request electronic copies (signed and dated, as appropriate) of the Entity's Facility ratings for all its applicable Facilities.
 - Ensure that the MLE is identified, as well as the second most limiting piece of equipment of each Facility
 - Ensure that Facility ratings reflect the ratings of relay protection devices as well as the impact of relay protection devices' trip settings on



- transmission Facilities' loadability (i.e.: PRC-023-4-Transmission Relay Loadability)
- Did the Entity provide Normal and Emergency Facility Ratings, as applicable?
 - In the NYISO and ISO-NE Control Areas, Emergency ratings must include Long Term Emergency (LTE) and Short Term Emergency (STE)
 - As the case may need, inquire whether Control Areas (other than the two above mentioned) require similar ratings.
- Ratings for Summer and Winter operating periods required at a minimum
- Basis for individual ratings and permitted duration of operation
- Ensure that re-ratings of, and modifications to, any existing equipment have been reflected in the current ratings.
- Request from the Entity a tabulation of BES Facilities (for all ratings in both operating periods) that shows "before" and "after" ratings, and calculations in percentages indicating increases/decrease for affected Facilities.
 - Establish # of noncompliant Facilities with incorrect equipment ratings
 - Establish # of Facilities with incorrect Facility Ratings
 - Facilities with incorrect Facility Ratings as a % the number of noncompliant Facilities
 - Facilities requiring derates as a % of the number of Facilities with incorrect Facility Ratings
 - Extent of adjustments needed for derates
- Determine the Entity's Extent of Condition (EOC) by ensuring that the Entity has had appropriate Facility ratings for earlier versions of the standard.
 - Verify compliance starting from June 18, 2007, the date when Standard FAC-009-1 (R1) became effective.
- Determine the duration of the noncompliance based on the date of the first incorrect Facility rating (or the first Facility rating reflecting an incorrect MLE), and the date when the last incorrect Facility rating (or the last Facility rating reflecting an incorrect MLE) was mitigated.
- Extent of Scope - If the Entity's Facility ratings were noncompliant, establish that the Entity has satisfied compliance requirements for R7 and R8 after mitigation of the R6 noncompliance.



R8 Scoping and Risk Determination

R8. Each TO (and each GO subject to Requirement R2) shall provide requested information as specified below (for its solely and jointly owned Facilities that are existing Facilities, new Facilities, modifications to existing Facilities and re-ratings of existing Facilities) to its associated Reliability Coordinator(s), Planning Coordinator(s), Transmission Planner(s), TOs and Transmission Operator(s): [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]

8.1 As scheduled by requesting entities:

8.1.1 Facility Ratings

8.1.2 Identity of the most limiting equipment of the Facilities

8.2 Within 30 calendar days (or a later date if specified by the requester), for any requested Facility with a Thermal Rating that limits the use of Facilities under the requester's authority by causing any of the following: 1) An Interconnection Reliability Operating Limit, 2) A limitation of Total Transfer Capability, 3) An impediment to generator deliverability, or 4) An impediment to service to a major load center:

8.2.1 Identity of the existing next most limiting equipment of the Facility

8.2.2 The Thermal Rating for the next most limiting equipment identified in Requirement R8, Part 8.2.1.

R8 Scope Evaluation

- Did the entity fail to provide its rating information to the requesting entity?
- Establish whether the entity:
 - o Provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by up to 15 days or more.
 - o Provided 100% or less of the required Rating information to the requesting entity.

Noncompliant with R8	Entity failed to provide requested information (for its solely and jointly owned Facilities that are existing Facilities, new Facilities, modifications to existing Facilities and re-ratings of existing Facilities) to its associated Reliability Coordinator(s), Planning Coordinator(s), Transmission Planner(s), TOs and Transmission Operator(s)
Noncompliant with R8, Part 8.1	Entity failed to provide requested information as scheduled by the requesting entities.
Noncompliant with R8, Part 8.1.1	Entity failed to provide Facility Ratings to its requesting entities.
Noncompliant with R8, Part 8.1.2	Entity failed to provide the identity of the most limiting equipment of the Facilities to its requesting entities.
Noncompliant with R8, Part 8.2	Entity failed to provide to its requesting entities information within 30 calendar days (or a later date if specified by the requester), for any requested Facility with a Thermal Rating that limits the use of Facilities under the requester's authority by causing any of the following: 1) An Interconnection Reliability Operating Limit, 2) A



	limitation of Total Transfer Capability, 3) An impediment to generator deliverability, or 4) An impediment to service to a major load center:
Noncompliant with R8, Part 8.2.1	Entity failed to provide the identity of the existing next most limiting equipment of the Facility to its requesting entities.
Noncompliant with R8, Part 8.2.2	Entity failed to provide the Thermal Rating for the next most limiting equipment identified in Requirement R8, Part 8.2.1. to its requesting entities

R8 Risk Determination

Risk Failure Statement: Noncompliance of FAC-008-5 R8 may cause an incorrect determination of Interconnection Reliability Operating Limits (IROLs), System Operating Limits (SOLs), Total Transfer Capability (TTC), generators' deliverability and may degrade service to major load centers.

Risk Criteria

- Identify the inherent properties of the Entity's noncompliant BES Facility(ies).
 - Generating Facility
 - Total output (MW)
 - Capacity Factor during the duration of the noncompliance
 - Classification as a critical resource or black-start unit
 - Variable resources (wind, solar, hydro)
 - Transmission Facility (if applicable)
 - Total customer load served/lost
 - Operating voltage (kV)
 - Part of IROLs or Inter-Area and Intra-Area interface(s)
 - Entity's Reliability Coordinator's required operating reserve
- Identify compensating controls/aggravating factors:
 - Does the entity monitor their equipment in real time?
 - Address the facility(ies)'s historical operation
 - Did the entity perform other Reliability assessments or Capacity tests?
 - Did the Reliability Coordinator or Transmission Operator have situation awareness of the most limiting element or the change in Facility Rating?
- Quality of internal compliance controls/procedures
 - Was the noncompliance self-identified
- Impact on Facility ratings
 - How many applicable BES Facilities were affected by the noncompliance?
 - Identify the number of Facilities requiring derates
 - Identify the extent of adjustment.
 - Identify if the component(s) at issue are the most limiting element (MLE) of the Facility
- Address duration
- Address actual harm.

Tier 3: Major BES Disturbances	Caused or contributed to a major BES disturbance
Tier 2: Moderate Impact	IROL exceeded, BES limit (non-IROL SOL, frequency, voltage, or ACE) exceeded for >30



	minutes, BES Facilities tripped unexpectedly, emergency action taken (e.g., reconfiguration, load shed) to mitigate or prevent the impact of the violation, equipment damage, major (>50%) loss of visibility, control, state estimation, or contingency analysis for over 30 minutes
Tier 1: Minor Impact	Observations similar to those in tier 2 but of lesser magnitude, or loss of ability to monitor cybersecurity intrusions.
Tier 0: No Impact	No observed impact.

R8 Mitigation Verification and Other Considerations

- Request the Entity to identify the data/information it failed to communicate to requesting entities and the specific process(es) (established by requesting entities) that was violated



NPCC Specific Details

- Transmission Planners
 - o ISO-New England
 - Winter Operating Reserve ~2600 MW
 - Summer Operating Reserve ~2200 MW
 - ISO-NE's most prominent process(es) for data submittal (annual and updates as they occur)
 - NX-9 process (see Sections II and IV of its OP-16 Procedure)
 - o New York Independent System Operator
 - Winter and Summer Operating Reserve ~1965 MW
 - NYISO most prominent process(es) for data submittal (annual and updates as they occur)
 - See Sections 2.1 and 2.2 of its RAD (Reliability Analysis Data) Manual
 - o New Brunswick
 - Winter and Summer: ~948 MW
- An applicable Facility is based on Entity-owned facilities located within the NPCC jurisdiction
- Phase Angle Regulators (PARs) help reduce the risk by modifying power flow distribution to resolve real time rating exceedances.

Enforcement Notes

- N/A



MOD-025-2 Enforcement Approach

Background Information

- [MOD-025-2 Standard Language](#)
- [MOD-025-2 Implementation Plan](#)

Standard/Implementation Plan Effective Dates

- **United States**

Standard	Requirement	Effective Date	% of Applicable Facilities
MOD-025-2	R1., R2., R3.	07/01/2016	40%
MOD-025-2	R1., R2., R3.	07/01/2017	60%
MOD-025-2	R1., R2., R3.	07/01/2018	80%
MOD-025-2	R1., R2., R3.	07/01/2019	100%

Key Terminology

Applicable Facilities:

- Individual generating unit greater than 20 MVA (gross nameplate rating) directly connected to the Bulk Electric System.
- Synchronous condenser greater than 20 MVA (gross nameplate rating) directly connected to the Bulk Electric System.
- Generating plant/Facility greater than 75 MVA (gross aggregate nameplate rating) directly connected to the Bulk Electric System.

Facility

A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)

Real Power

The portion of electricity that supplies energy to the load

Reactive Power

The portion of electricity that establishes and sustains the electric and magnetic fields of alternating-current equipment. Reactive Power must be supplied to most types of magnetic equipment, such as motors and transformers. It also must supply the reactive losses on transmission facilities. Reactive Power is provided by generators, synchronous



NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

condensers, or electrostatic equipment such as capacitors and directly influences electric system voltage. It is usually expressed in kilovars (kvar) or megavars (Mvar).



R1 Scoping and Risk Determination

R1. Each Generator Owner shall provide its Transmission Planner with verification of the Real Power capability of its applicable Facilities as follows:

1.1. Verify the Real Power capability of its generating units in accordance with Attachment 1.

1.2. Submit a completed Attachment 2 (or a form containing the same information as identified in Attachment 2) to its Transmission Planner within 90 calendar days of either (i) the date the data is recorded for a staged test; or (ii) the date the data is selected for verification using historical operational data.

R1 Scope Evaluation

Noncompliant with R1.1	Entity failed to verify Real Power capability within the periodicity and/or parameters in Attachment 1
Noncompliant with R1.2	Entity failed to submit a completed Attachment 2 form related to Real Power capability.
Noncompliant with R1.2	Entity failed to submit Attachment 2 forms within 90 days of either (i) the date the data was recorded for a staged test or (ii) the date the data was selected for verification using historical operational data

- How many applicable Facilities were noncompliant?

R1 Risk Determination

Risk Failure Statement: Noncompliance with MOD-025-2 R1 reduces the accuracy of the Transmission Planner's models and planning studies used to assess system reliability.

Risk Criteria

- Identify the inherent properties of the applicable facilities
 - Total output (MW or MVA)
 - Capacity Factor within the duration of the noncompliance
 - Classification as a black-start resource
 - Entity's Reliability Coordinator operating reserve
- Establish the duration of the noncompliance
- Has the entity provided or required to provide Real Power capability testing data to the Transmission Planner?
 - Identify differences between the entity's submittal and the Standard/Requirement
 - ***NOTE: ISONE and NYISO require each GO to provide capability data on a seasonable basis. Ask the entity to provide you with the capability data.



NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

- What were the results of the Real Power capability tests?
 - Did the Real Power capability change since the last submittal?
- Address actual harm

Tier 3: Major BES Disturbances	Caused or contributed to a major BES disturbance
Tier 2: Moderate Impact	IROL exceeded, BES limit (non-IROL SOL, frequency, voltage, or ACE) exceeded for >30 minutes, BES Facilities tripped unexpectedly, emergency action taken (e.g., reconfiguration, load shed) to mitigate or prevent the impact of the violation, equipment damage, major (>50%) loss of visibility, control, state estimation, or contingency analysis for over 30 minutes
Tier 1: Minor Impact	Observations similar to those in tier 2 but of lesser magnitude, or loss of ability to monitor cybersecurity intrusions.
Tier 0: No Impact	No observed impact.

R1 Mitigation Verification

- For Verification Check common places of disparity
 - Did the real power test last for over an hour? Did they document the start and end time?
 - Make sure Hydrogen pressure is recorded, if not, ask if Generator is Hydrogen cooled. Normally, >150MW is usually hydrogen cooled.
 - Attachment 2 specifically asks data for “Generator hydrogen pressure at time of test”
 - Solar and Wind must have at least 90% of their units on for a valid test
 - Ambient temps have NO impact on solar or hydro, so willing to overlook if they don’t record that in the data submittals.
 - Check email address correct for form submittals. Any confirmation from ISOs upon receipt?
 - All generators, no matter what type, must complete real power verification tests.



R2 Scoping and Risk Determination

R2. Each Generator Owner shall provide its Transmission Planner with verification of the Reactive Power capability of its applicable Facilities as follows:

2.1. Verify, in accordance with Attachment 1, (i) the Reactive Power capability of its generating units and (ii) the Reactive Power capability of its synchronous condenser units.

2.2. Submit a completed Attachment 2 (or a form containing the same information as identified in Attachment 2) to its Transmission Planner within 90 calendar days of either (i) the date the data is recorded for a staged test; or (ii) the date the data is selected for verification using historical operational data.

R2 Scope Evaluation

Noncompliant with R2.1	Entity failed to verify Reactive Power capability within the periodicity and/or parameters in Attachment 1
Noncompliant with R2.2	Entity failed to submit a completed Attachment 2 form related to Reactive Power capability.
Noncompliant with R2.2	Entity failed to submit Attachment 2 forms within 90 days of either (i) the date the data was recorded for a staged test or (ii) the date the data was selected for verification using historical operational data

- How many applicable Facilities does the entity own?

R2 Risk Determination

Risk Failure Statement: Noncompliance with MOD-025-2 R2 reduces the accuracy of the Transmission Planner's models and planning studies used to assess system reliability.

Risk Criteria

- Identify the inherent properties of the entity
 - Total output (MW or MVA)
 - Capacity Factor
 - Classification as a black-start resource
 - Reliability Coordinator operating reserve
- Establish the duration of the noncompliance
- Has the entity provided or required to provide other Reactive Power capability testing data to the Transmission Planner?



NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

- Identify differences between the entity's submittal and the Standard/Requirement
- ***NOTE: ISONE and NYISO require each GO to provide capability data on a seasonable basis. Ask the entity to provide you with the capability data.
- What were the results of the Reactive Power capability tests?
 - Did the Reactive Power capability change?
- Address actual harm

Tier 3: Major BES Disturbances	Caused or contributed to a major BES disturbance
Tier 2: Moderate Impact	IROL exceeded, BES limit (non-IROL SOL, frequency, voltage, or ACE) exceeded for >30 minutes, BES Facilities tripped unexpectedly, emergency action taken (e.g., reconfiguration, load shed) to mitigate or prevent the impact of the violation, equipment damage, major (>50%) loss of visibility, control, state estimation, or contingency analysis for over 30 minutes
Tier 1: Minor Impact	Observations similar to those in tier 2 but of lesser magnitude, or loss of ability to monitor cybersecurity intrusions.
Tier 0: No Impact	No observed impact.

R2 Mitigation Verification

- For Verification Check common places of disparity
 - Make sure H2 is recorded, if not, ask if Generator is H2 cooled? >150MW is usually H2 cooled.
 - Solar and Wind must have at least 90% of their units on for a valid test
 - Ambient temps have NO impact on solar or hydro. Not NECESSARY in the data submittals.
 - Check email address correct for form submittals. Any confirmation from ISOs upon receipt?
- Four Tests that Need to be done
 - Full/Max Power
 - Max Lag
 - Max Lead
 - Low/Min Power
 - Max Lag
 - Max Lead
- EXCLUSION to the above statement:



NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

- NUKES – At Max real do Max lag and Max lead (2 tests) – can be separate, but normally you do max real and max lag at same time, if so... see R1 – make sure the test is done over an hour.
 - NO tests are done at min power.
- WIND & SOLAR – one test (R1) max real with max lag: remember has to be 90% of the units.



R3 Scoping and Risk Determination

R3. Each Transmission Owner shall provide its Transmission Planner with verification of the Reactive Power capability of its applicable Facilities as follows:

- 3.1.** Verify, in accordance with Attachment 1, the Reactive Power capability of its synchronous condenser units.
- 3.2.** Submit a completed Attachment 2 (or a form containing the same information as identified in Attachment 2) to its Transmission Planner within 90 calendar days of either (i) the date the data is recorded for a staged test; or (ii) the date the data is selected for verification using historical operational data.

R3 Scope Evaluation

Noncompliant with R3.1	Entity failed to verify Reactive Power capability within the periodicity and/or parameters in Attachment 1
Noncompliant with R3.2	Entity failed to complete all Reactive Power capability data fields according to Attachment 2
Noncompliant with R3.2	Entity failed to submit Attachment 2 forms for each applicable generating unit to its Transmission Planner within 90 days of either the date the data was recorded for a staged test or the date the data was selected for verification using historical operational data

- How many applicable Facilities does the entity own?

Risk Determination

Risk Failure Statement: Noncompliance with MOD-025-2 R3 reduces the accuracy of the Transmission Planner's models and planning studies used to assess system reliability.

Risk Criteria

- Identify the inherent properties of the entity
 - Reactive Power (MVAR)
 - Classification as an IROL
- Establish the duration of the noncompliance
- Has the entity provided or required to provide other Reactive Power capability testing data to the Transmission Planner?
 - Identify differences between the entity's submittal and the Standard/Requirement



NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

- ***NOTE: ISONE and NYISO require each GO to provide capability data on a seasonable basis. Ask the entity to provide you with the capability data.
- What were the results of the reactive power capability tests?
 - Did the Reactive Power capability change?
- Address actual harm

Tier 3: Major BES Disturbances	Caused or contributed to a major BES disturbance
Tier 2: Moderate Impact	IROL exceeded, BES limit (non-IROL SOL, frequency, voltage, or ACE) exceeded for >30 minutes, BES Facilities tripped unexpectedly, emergency action taken (e.g., reconfiguration, load shed) to mitigate or prevent the impact of the violation, equipment damage, major (>50%) loss of visibility, control, state estimation, or contingency analysis for over 30 minutes
Tier 1: Minor Impact	Observations similar to those in tier 2 but of lesser magnitude, or loss of ability to monitor cybersecurity intrusions.
Tier 0: No Impact	No observed impact.

NPCC Specific Details

- NPCC Transmission Planners (ISO-NE and NYISO) request capability data using different forms than Attachment 2. An example form that is inconsistent with the standard is the Demonstrated Maximum Net Capability (DMNC) used and submitted annually to NYISO. The TP request form does NOT contain the same amount of information as attachment 2. The GO/TO is noncompliant if the GO/TO submits ONLY the TP form.
- Transmission Planners
 - ISO-New England
 - [2021 ISONE MOD-025-2 Bulletin](#)
 - Winter Operating Reserve ~2600 MW
 - Summer Operating Reserve ~2200 MW
 - Historically, ISO-NE submission form was missing End Time and One-Line
 - New York Independent System Operator
 - Winter and Summer Operating Reserve ~1965 MW
 - New Brunswick
 - Winter and Summer: ~948 MW



NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

Enforcement Notes



PRC-005-6 Enforcement Approach

Background Information

- [PRC-005-6 Standard Language](#)
- [PRC-005-6 Implementation Plan](#)

Standard/Implementation Plan Effective Dates

United States

Standard	Requirement	Effective Date
PRC-005-6	R1., R2., R3., R4., R5	01/01/2016
PRC-005-6	R3., R4.	See R3 Scope for Implementation Plan Details

Quebec

Applicable Functions:

- Transmission Owner (TO)
- Generator Owner (GO)
- Distribution Provider (DP)

Applicable Facilities:

1. Protection Systems and Sudden Pressure Relaying that are installed for the purpose of detecting Faults on BES Elements (lines, buses, transformers, etc.)
2. Protection Systems used for underfrequency load-shedding systems installed per ERO underfrequency load-shedding requirements.
3. Protection Systems used for undervoltage load-shedding systems installed to prevent system voltage collapse or voltage instability for BES reliability.
4. Protection Systems installed as a Remedial Action Scheme (RAS) for BES reliability.
5. Protection Systems and Sudden Pressure Relaying for generator Facilities that are part of the BES, except for generators identified through Inclusion I4 of the BES definition, including:
 - 5.1. Protection Systems that act to trip the generator either directly or via lockout or auxiliary tripping relays.
 - 5.2. Protection Systems and Sudden Pressure Relaying for generator step-up transformers for generators that are part of the BES.
 - 5.3. Protection Systems and Sudden Pressure Relaying for station service or excitation transformers connected to the generator bus of generators which



are part of the BES, that act to trip the generator either directly or via lockout or tripping auxiliary relays.

6. Protection Systems and Sudden Pressure Relaying for the following BES generator Facilities for dispersed power producing resources identified through Inclusion I4 of the BES definition:
 - 6.1. Protection Systems and Sudden Pressure Relaying for Facilities used in aggregating dispersed BES generation from the point where those resources aggregate to greater than 75 MVA to a common point of connection at 100kV or above.
7. Automatic Reclosing¹, including:
 - 7.1. Automatic Reclosing applied on the terminals of Elements connected to the BES bus located at generating plant substations where the total installed gross generating plant capacity is greater than the gross capacity of the largest BES generating unit within the Balancing Authority Area or, if a member of a Reserve Sharing Group, the largest generating unit within the Reserve Sharing Group.²
 - 7.2. Automatic Reclosing applied on the terminals of all BES Elements at substations one bus away from generating plants specified in Section 7.1 when the substation is less than 10 circuit-miles from the generating plant substation.
 - 7.3. Automatic Reclosing applied as an integral part of an RAS specified in Section 4.

Key Terminology

Automatic Reclosing – Includes the following Components:

- Reclosing relay
- Supervisory relay(s) or function(s) – relay(s) or function(s) that perform voltage and/or sync check functions that enable or disable operation of the reclosing relay
- Voltage sensing devices associated with the supervisory relay(s) or function(s)
- Control circuitry associated with the reclosing relay or supervisory relay(s) or function(s)

Sudden Pressure Relaying – A system that trips an interrupting device(s) to isolate the equipment it is monitoring and includes the following Components:

¹ Automatic Reclosing addressed in Section 7.1 and 7.2 may be excluded if the equipment owner can demonstrate that a close-in three-phase fault present for twice the normal clearing time (capturing a minimum trip-close-trip time delay) does not result in a total loss of gross generation in the Interconnection exceeding the gross capacity of the largest relevant BES generating unit where the Automatic Reclosing is applied.

² The largest BES generating unit within the Balancing Authority Area or the largest generating unit within the Reserve Sharing Group, as applicable, is subject to change. As a result of such a change, the Automatic Reclosing Components subject to the standard could change effective on the date of such change.



- Fault pressure relay – a mechanical relay or device that detects rapid changes in gas pressure, oil pressure, or oil flow that are indicative of Faults within liquid-filled, wire-wound equipment
- Control circuitry associated with a fault pressure relay

Unresolved Maintenance Issue – A deficiency identified during a maintenance activity that causes the Component to not meet the intended performance, cannot be corrected during the maintenance interval, and requires follow-up corrective action.

Segment – Components of a consistent design standard, or a particular model or type from a single manufacturer that typically share other common elements. Consistent performance is expected across the entire population of a Segment. A Segment must contain at least sixty (60) individual Components.

Component Type –

- Any one of the five specific elements of a Protection System
- Any one of the four specific elements of Automatic Reclosing
- Any one of the two specific elements of Sudden Pressure Relaying

Component – Any individual discrete piece of equipment included in a Protection System, Automatic Reclosing, or Sudden Pressure Relaying.

Countable Event – A failure of a Component requiring repair or replacement, any condition discovered during the maintenance activities in Tables 1-1 through 1-5, Table 3, Tables 4-1 through 4-3, and Table 5, which requires corrective action or a Protection System Misoperation attributed to hardware failure or calibration failure. Misoperations due to product design errors, software errors, relay settings different from specified settings, Protection System Component, Automatic Reclosing, or Sudden Pressure Relaying configuration or application errors are not included in Countable Events.



R1 Scoping and Risk Determination

R1. Each TO, GO and DP shall establish a Protection System Maintenance Program (PSMP) for its Protection Systems, Automatic Reclosing, and Sudden Pressure Relaying identified in Section 4.2, Facilities. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].

The PSMP shall:

- 1.1. Identify which maintenance method (time-based, performance-based per PRC-005 Attachment A, or a combination) is used to address each Protection System, Automatic Reclosing, and Sudden Pressure Relaying Component Type. All batteries associated with the station dc supply Component Type of a Protection System shall be included in a time-based program as described in Table 1-4 and Table 3.
- 1.2. Include the applicable monitored Component attributes applied to each Protection System, Automatic Reclosing, and Sudden Pressure Relaying Component Type consistent with the maintenance intervals specified in [Tables 1-1](#) through [1-5](#), [Table 2](#), [Table 3](#), [Table 4-1](#) through [4-3](#), and [Table 5](#) where monitoring is used to extend the maintenance intervals beyond those specified for unmonitored Protection System, Automatic Reclosing, and Sudden Pressure Relaying Components.

R1 Scope Evaluation

Noncompliant with R1	Entity failed to establish a Protection System Maintenance Program (PSMP) for its Protection Systems, Automatic Reclosing, and Sudden Pressure Relaying identified in Section 4.2., Facilities.
Noncompliant with R1, Part 1.1	Entity's PSMP failed to identify whether one or more Protection System, Automatic Reclosing, and Sudden Pressure Relaying Component Type(s) are being addressed by time-based, performance-based, or a combination of both maintenance methods.
Noncompliant with R1, Part 1.1	Entity's PSMP failed to include applicable station batteries in a time-based maintenance program.
Noncompliant with R1, Part 1.2	Entity's PSMP failed to include all applicable monitored component attributes applied to each Protection System, Automatic Reclosing, and Sudden Pressure Relaying Component Type consistent with the maintenance intervals as described in the Standard.

- How many component type(s) is (are) missing or otherwise noncompliant (e.g.: missing maintenance method utilized for testing, missing component attributes, etc.)?



- How many components are missing or otherwise noncompliant for each applicable component type?
 - o Specify which component(s) were noncompliant because they had missing maintenance activity(ies), testing intervals and their basis, summary of required activities, etc. (see example below).
 - o Determine the percentage of noncompliant/missing components with respect to the baseline applicable component for the affected component type(s)
- Determine the Entity's Extent of Condition (EOC) by ensuring that the Entity has had an appropriate Protection System Maintenance Program (PSMP) document for the various versions of the standard, as applicable.
 - o Verify compliance starting from November 25, 2013, the date when Standard PRC-005-1.1b became effective. This early version of the standard is still in effect through March 31, 2027.
 - o Establish when the Entity first adopted a Time-based performance testing for its noncompliant component(s) or component type(s)
- Determine the duration of the noncompliance based on: Implementation Plan(s)' timelines (when applicable), missed PSMP documentation, missed component type(s), and/or missed component(s), etc.

Component type(s)	Maintenance Table(s)	Component Attributes	Maximum Maintenance Interval(s)	Missed Maintenance Activity(ies)
VLA Batteries	Table 1-4(a)	Protection System Station dc supply using Vented Lead-Acid (VLA) batteries not having monitoring attributes of Table 1-4(f).	18 Calendar Months	Battery terminal connection resistance
Protective Relay excluding distributed UFLS and distributed UVLS	Table 1-1	Any unmonitored protective relay not having all the monitoring attributes of a category below	6 Calendar Years	Verify acceptable measurement of power system input values.

R1 Risk Determination

Risk Failure Statement:

Noncompliance with PRC-005-6 R1 increases the risk of components failing to operate when needed due to a failure to properly maintain protection system components.

Risk Criteria

- Identify the inherent properties of the applicable Facilities:
 - o Generating Facility
 - Total output (MW)
 - Capacity Factor
 - Classification as a black-start unit
 - Entity's Reliability Coordinator operating reserve



- Transmission Facility
 - Total customer load served/lost
 - Operating voltage (kV)
 - Part of IROLs or Inter-Area and Intra-Area interface(s)
 - Entity's Reliability Coordinator's (RC) required operating reserve
- Identify whether the entity had any compensating controls (e.g., self-monitoring devices, equipment redundancy, alarms)
- How many of the Entity's BES Facilities are part of the applicable baseline facilities?
 - How many applicable BES Facilities were affected by the noncompliance?
- Address any misoperations during the noncompliant duration
- Adequacy of internal controls/procedures
- Determine whether actual harm has occurred (see categories below).

Tier 3: Major BES Disturbances	Caused or contributed to a major BES disturbance
Tier 2: Moderate Impact	IROL exceeded, BES limit (non-IROL SOL, frequency, voltage, or ACE) exceeded for >30 minutes, BES Facilities tripped unexpectedly, emergency action taken (e.g., reconfiguration, load shed) to mitigate or prevent the impact of the violation, equipment damage, major (>50%) loss of visibility, control, state estimation, or contingency analysis for over 30 minutes
Tier 1: Minor Impact	Observations similar to those in tier 2 but of lesser magnitude, or loss of ability to monitor cybersecurity intrusions.
Tier 0: No Impact	No observed impact.

R1 Mitigation Verification

- For verification



R2 Scoping and Risk Determination

R2. Each TO, GO, and DP that uses performance-based maintenance intervals in its PSMP shall follow the procedure established in PRC-005 Attachment A to establish and maintain its performance-based intervals. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]



R3 Scoping and Risk Determination

R3. Each TO, GO, and DP that utilizes time-based maintenance program(s) shall maintain its Protection System, Automatic Reclosing, and Sudden Pressure Relaying Components that are included within the time-based maintenance program in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within [Tables 1-1](#) through [1-5](#), [Table 2](#), [Table 3](#), [Table 4-1](#) through [4-3](#), and [Table 5](#). [Violation Risk Factor: High] [Time Horizon: Operations Planning]

R3 United States Implementation Plan

For Component Types in PRC-005-2

Max Maintenance Interval	% Compliant	By
Less than 1 year	100%	October 1, 2015
1-2 Calendar Years	100%	April 1, 2017

Max Maintenance Interval	% Compliant	By
3 Calendar years	30	April 1, 2016
3 Calendar years	60	April 1, 2017
3 Calendar years	100	April 1, 2018

Max Maintenance Interval	% Compliant	By
6 Calendar years	30	April 1, 2017
6 Calendar years	60	April 1, 2019
6 Calendar years	100	April 1, 2021

Max Maintenance Interval	% Compliant	By
12 Calendar years	30	April 1, 2019
12 Calendar years	60	April 1, 2023
12 Calendar years	100	April 1, 2027

For Component Types added in PRC-005-6 (Automatic Reclosing Components, Sudden Pressure Relaying Components, and dispersed generation resources)

Max Maintenance Interval	% Compliant	By
6 Calendar years	30	January 1, 2019
6 Calendar years	60	January 1, 2021
6 Calendar years	100	January 1, 2023



Max Maintenance Interval	% Compliant	By
12 Calendar years	30	January 1, 2021
12 Calendar years	60	January 1, 2025
12 Calendar years	100	January 1, 2029



R3 Scope Evaluation

Noncompliant with R3	Entity failed to meet the compliant percentage by the implementation plan timelines.
Noncompliant with R3	Entity failed to maintain components within the component type's maximum maintenance intervals prescribed in Tables 1-1 through 1-5 , Table 2 , Table 3 , Table 4-1 through 4-3 , and Table 5 .

- How many components are missing or otherwise noncompliant for each applicable component type?
 - o Address the Entity's Extent of Condition (EOC)
- Specify which component type(s) were noncompliant from [Tables 1-1](#) through [1-5](#), [Table 2](#), [Table 3](#), [Table 4-1](#) through [4-3](#), and/or [Table 5](#).
 - o Identify the missing maintenance activity(ies),
 - o Identify the maximum maintenance intervals,
 - o Determine the percentage of noncompliant/missing components with respect to the baseline applicable component for the affected component type(s)
- Determine the duration of the noncompliance based on: Implementation Plan(s)' timelines (when applicable) or missed maintenance interval

PRC-005-6 R3 Scope Example

Component type(s)	Maintenance Table(s)	Component Attributes	Maximum Maintenance Interval(s)	Missed Maintenance Activity(ies)
Vented Lead-Acid Batteries	Table 1-4(a)	Protection System Station dc supply using Vented Lead-Acid (VLA) batteries not having monitoring attributes of Table 1-4(f).	18 Calendar Months	Battery terminal connection resistance
Protective Relay excluding distributed UFLS and distributed UVLS	Table 1-1	Any unmonitored protective relay not having all the monitoring attributes of a category below	6 Calendar Years	Verify acceptable measurement of power system input values.



R3 Risk Determination

Risk Failure Statement:

Noncompliance with PRC-005-6 R3 may deteriorate protection systems' performance. Inadequate operation of protection systems may, in turn, cause generating/transmission facilities to trip unnecessarily or, conversely, cause damage to electrical equipment by prolonging exposure to electrical faults not cleared within design time parameters.

Risk Criteria

- How many of the Entity's BES Facilities are part of the baseline applicable facilities?
 - How many applicable BES Facilities were affected by this noncompliance?
- Address the condition of noncompliant components after the noncompliance was been mitigated
- Address the noncompliant components
 - Include any compensating controls (e.g., self-monitoring devices, equipment redundancy, alarms)
 - Include any tests that were performed
- Identify the inherent properties of the noncompliant BES Facility(ies)
 - Generating Facility(ies)
 - Active Power output (MW)
 - Capacity Factor within the duration of the noncompliance
 - Classification as a critical resource or black-start unit
 - Variable resources (wind, solar)
 - Transmission Facility
 - Total customer load served/lost
 - Operating Voltage (kV)
 - Part of IROLs or Inter-Area interface(s)
 - Entity's Reliability Coordinator's Required Operating Reserve
- Determine harm whether actual harm has occurred (see categories below).

Tier 3: Major BES Disturbances	Caused or contributed to a major BES disturbance
Tier 2: Moderate Impact	IROL exceeded, BES limit (non-IROL SOL, frequency, voltage, or ACE) exceeded for >30 minutes, BES Facilities tripped unexpectedly, emergency action taken (e.g., reconfiguration, load shed) to mitigate or prevent the impact of the violation, equipment damage, major (>50%) loss of visibility, control, state estimation, or contingency analysis for over 30 minutes
Tier 1: Minor Impact	Observations similar to those in tier 2 but of lesser magnitude, or loss of ability to monitor cybersecurity intrusions.



Tier 0: No Impact

No observed impact.

R3 Mitigation Verification or Higher Risk considerations

- Ensure the entity reviewed historical testing records of its applicable protection system components with due consideration to the implementation plan
- Ensure that the entity reviewed historical records
- When did the entity first adopt a time-based performance testing for its noncompliant component types?



R4 Scoping and Risk Determination

R4. Each TO, GO, and DP that utilizes performance-based maintenance program(s) in accordance with Requirement R2 shall implement and follow its PSMP for its Protection System, Automatic Reclosing, and Sudden Pressure Relaying Components that are included within the performance-based program(s). [Violation Risk Factor: High] [Time Horizon: Operations Planning].

Note: all Registered Entities within NPCC utilize time-based maintenance program(s)



R5 Scoping and Risk Determination

R5. Each TO, GO, and DP shall demonstrate efforts to correct identified Unresolved Maintenance Issues. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].

R5 Scope Evaluation

Noncompliant with R5	Entity failed to demonstrate efforts correct the identified Unresolved Maintenance Issues
----------------------	---

- How many components are part of the baseline component type(s) affected by the noncompliance?
 - o Address the Entity's Extent of Condition (EOC)
 - How many Unresolved Maintenance Issues has the Entity failed to identify?
 - How many Unresolved Maintenance Issues have been identified for which the Entity failed to undertake efforts to correct?
 - How many protection components were noncompliant?

R5 Risk Determination

Risk Failure Statement:

The Entity's failure to identify Unresolved Maintenance Issues (UMI) could delay efforts to correct issues in a timely manner, and cause protection systems to not operate as designed. This could result in unnecessary tripping of system facilities or damage to electrical equipment when electrical faults are not cleared per design.

Risk Criteria

- o Address the condition of untested equipment after the noncompliance has been mitigated
- o Include any compensating controls (e.g., self-monitoring devices, equipment redundancy, alarms)
- o How many BES Facilities are part of the Entity's baseline applicable facilities?
 - How many applicable BES Facilities were affected by the noncompliance?
- o Identify the inherent properties of the noncompliant BES Facility(ies)
 - Generating Facility(ies)
 - Active Power output (MW)
 - Capacity Factor within the duration of the noncompliance
 - Classification as a critical resource or black-start unit
 - Transmission Facility
 - Total customer load served/lost
 - Operating Voltage (kV)
 - Part of IROLs or Inter-Area interface(s)



- Entity's Reliability Coordinator's Required Operating Reserve
 - Determine whether actual harm has occurred (see categories below).

Tier 3: Major BES Disturbances	Caused or contributed to a major BES disturbance
Tier 2: Moderate Impact	IROL exceeded, BES limit (non-IROL SOL, frequency, voltage, or ACE) exceeded for >30 minutes, BES Facilities tripped unexpectedly, emergency action taken (e.g., reconfiguration, load shed) to mitigate or prevent the impact of the violation, equipment damage, major (>50%) loss of visibility, control, state estimation, or contingency analysis for over 30 minutes
Tier 1: Minor Impact	Observations similar to those in tier 2 but of lesser magnitude, or loss of ability to monitor cybersecurity intrusions.
Tier 0: No Impact	No observed impact.



NPCC Specific Details

- Transmission Planners
 - o ISO-New England
 - Historical All-time Summer Peak ~ 28,100 MW
 - Historical All-time Winter Peak ~ 22,800 MW
 - Winter Required Operating Reserve ~2400 MW
 - Summer Required Operating Reserve ~2200 MW
 - o New York Independent System Operator
 - Historical All-time Summer Peak ~ 34,000 MW
 - Historical All-time Winter Peak ~ 25,700 MW
 - Winter and Summer Required Operating Reserve ~1965 MW
- An applicable Facility is based on Entity-owned facilities located within the NPCC jurisdiction

Enforcement Notes

- To be determined

Table 1-1 Component Type - Protective Relay Excluding distributed UFLS and distributed UVLS (see Table 3)		
Component Attributes	Maximum Maintenance Interval ³	Maintenance Activities
Any unmonitored protective relay not having all the monitoring attributes of a category below.	6 Calendar Years	<p>For all unmonitored relays:</p> <ul style="list-style-type: none"> • Verify that settings are as specified <p>For non-microprocessor relays:</p> <ul style="list-style-type: none"> • Test and, if necessary calibrate <p>For microprocessor relays:</p> <ul style="list-style-type: none"> • Verify operation of the relay inputs and outputs that are essential to proper functioning of the Protection System. • Verify acceptable measurement of power system input values.
<p>Monitored microprocessor protective relay with the following:</p> <ul style="list-style-type: none"> • Internal self-diagnosis and alarming (see Table 2). • Voltage and/or current waveform sampling three or more times per power cycle, and conversion of samples to numeric values for measurement calculations by microprocessor electronics. • Alarming for power supply failure (see Table 2). 	12 Calendar Years	<p>Verify:</p> <ul style="list-style-type: none"> • Settings are as specified. • Operation of the relay inputs and outputs that are essential to proper functioning of the Protection System. • Acceptable measurement of power system input values.

³ For the tables in this standard, a calendar year starts on the first day of a new year (January 1) after a maintenance activity has been completed.
For the tables in this standard, a calendar month starts on the first day of the first month after a maintenance activity has been completed.

Table 1-1 Component Type - Protective Relay Excluding distributed UFLS and distributed UVLS (see Table 3)		
Component Attributes	Maximum Maintenance Interval³	Maintenance Activities
<p>Monitored microprocessor protective relay with preceding row attributes and the following:</p> <ul style="list-style-type: none"> • Ac measurements are continuously verified by comparison to an independent ac measurement source, with alarming for excessive error (See Table 2). • Some or all binary or status inputs and control outputs are monitored by a process that continuously demonstrates ability to perform as designed, with alarming for failure (See Table 2). • Alarming for change of settings (See Table 2). 	12 Calendar Years	Verify only the unmonitored relay inputs and outputs that are essential to proper functioning of the Protection System.

Table 1-2 Component Type - Communications Systems Excluding distributed UFLS and distributed UVLS (see Table 3)		
Component Attributes	Maximum Maintenance Interval	Maintenance Activities
Any unmonitored communications system necessary for correct operation of protective functions, and not having all the monitoring attributes of a category below.	4 Calendar Months	Verify that the communications system is functional.
	6 Calendar Years	Verify that the communications system meets performance criteria pertinent to the communications technology applied (e.g. signal level, reflected power, or data error rate). Verify operation of communications system inputs and outputs that are essential to proper functioning of the Protection System.
Any communications system with continuous monitoring or periodic automated testing for the presence of the channel function, and alarming for loss of function (See Table 2).	12 Calendar Years	Verify that the communications system meets performance criteria pertinent to the communications technology applied (e.g. signal level, reflected power, or data error rate). Verify operation of communications system inputs and outputs that are essential to proper functioning of the Protection System.
Any communications system with all of the following: <ul style="list-style-type: none"> Continuous monitoring or periodic automated testing for the performance of the channel using criteria pertinent to the communications technology applied (e.g. signal level, reflected power, or data error rate, and alarming for excessive performance degradation). (See Table 2) Some or all binary or status inputs and control outputs are monitored by a process that continuously demonstrates ability to perform as designed, with alarming for failure (See Table 2). 	12 Calendar Years	Verify only the unmonitored communications system inputs and outputs that are essential to proper functioning of the Protection System

Table 1-3 Component Type - Voltage and Current Sensing Devices Providing Inputs to Protective Relays Excluding distributed UFLS and distributed UVLS (see Table 3)		
Component Attributes	Maximum Maintenance Interval	Maintenance Activities
Any voltage and current sensing devices not having monitoring attributes of the category below.	12 Calendar Years	Verify that current and voltage signal values are provided to the protective relays.
Voltage and Current Sensing devices connected to microprocessor relays with ac measurements that are continuously verified by comparison of sensing input value, as measured by the microprocessor relay, to an independent ac measurement source, with alarming for unacceptable error or failure (see Table 2).	No periodic maintenance specified	None.

<p>Table 1-4(a)</p> <p>Component Type – Protection System Station dc Supply Using Vented Lead-Acid (VLA) Batteries</p> <p>Excluding distributed UFLS and distributed UVLS (see Table 3)</p> <p>Protection System Station dc supply used only for non-BES interrupting devices for RAS, non-distributed UFLS systems, or non-distributed UVLS systems is excluded (see Table 1-4(e)).</p>		
Component Attributes	Maximum Maintenance Interval	Maintenance Activities
Protection System Station dc supply using Vented Lead-Acid (VLA) batteries not having monitoring attributes of Table 1-4(f).	4 Calendar Months	<p>Verify:</p> <ul style="list-style-type: none"> • Station dc supply voltage <p>Inspect:</p> <ul style="list-style-type: none"> • Electrolyte level • For unintentional grounds
	18 Calendar Months	<p>Verify:</p> <ul style="list-style-type: none"> • Float voltage of battery charger • Battery continuity • Battery terminal connection resistance • Battery intercell or unit-to-unit connection resistance <p>Inspect:</p> <ul style="list-style-type: none"> • Cell condition of all individual battery cells where cells are visible – or measure battery cell/unit internal ohmic values where the cells are not visible • Physical condition of battery rack

Table 1-4(a)

Component Type – Protection System Station dc Supply Using Vented Lead-Acid (VLA) Batteries
Excluding distributed UFLS and distributed UVLS (see Table 3)

Protection System Station dc supply used only for non-BES interrupting devices for RAS, non-distributed UFLS systems, or non-distributed UVLS systems is excluded (see Table 1-4(e)).

Component Attributes	Maximum Maintenance Interval	Maintenance Activities
	<p>18 Calendar Months</p> <p>-or-</p> <p>6 Calendar Years</p>	<p>Verify that the station battery can perform as manufactured by evaluating cell/unit measurements indicative of battery performance (e.g. internal ohmic values or float current) against the station battery baseline.</p> <p>-or-</p> <p>Verify that the station battery can perform as manufactured by conducting a performance or modified performance capacity test of the entire battery bank.</p>

<p>Table 1-4(b)</p> <p>Component Type – Protection System Station dc Supply Using Valve-Regulated Lead-Acid (VRLA) Batteries</p> <p>Excluding distributed UFLS and distributed UVLS (see Table 3)</p> <p>Protection System Station dc supply used only for non-BES interrupting devices for RAS, non-distributed UFLS systems, or non-distributed UVLS systems is excluded (see Table 1-4(e)).</p>		
Component Attributes	Maximum Maintenance Interval	Maintenance Activities
Protection System Station dc supply with Valve Regulated Lead-Acid (VRLA) batteries not having monitoring attributes of Table 1-4(f).	4 Calendar Months	Verify: <ul style="list-style-type: none"> • Station dc supply voltage Inspect: <ul style="list-style-type: none"> • For unintentional grounds
	6 Calendar Months	Inspect: <ul style="list-style-type: none"> • Condition of all individual units by measuring battery cell/unit internal ohmic values.
	18 Calendar Months	Verify: <ul style="list-style-type: none"> • Float voltage of battery charger • Battery continuity • Battery terminal connection resistance • Battery intercell or unit-to-unit connection resistance Inspect: <ul style="list-style-type: none"> • Physical condition of battery rack

Table 1-4(b)

**Component Type – Protection System Station dc Supply Using Valve-Regulated Lead-Acid (VRLA) Batteries
Excluding distributed UFLS and distributed UVLS (see Table 3)**

Protection System Station dc supply used only for non-BES interrupting devices for RAS, non-distributed UFLS systems, or non-distributed UVLS systems is excluded (see Table 1-4(e)).

Component Attributes	Maximum Maintenance Interval	Maintenance Activities
	6 Calendar Months -or- 3 Calendar Years	Verify that the station battery can perform as manufactured by evaluating cell/unit measurements indicative of battery performance (e.g. internal ohmic values or float current) against the station battery baseline. -or- Verify that the station battery can perform as manufactured by conducting a performance or modified performance capacity test of the entire battery bank.

Table 1-4(c) Component Type – Protection System Station dc Supply Using Nickel-Cadmium (NiCad) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for RAS, non-distributed UFLS system, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	Maximum Maintenance Interval	Maintenance Activities
Protection System Station dc supply Nickel-Cadmium (NiCad) batteries not having monitoring attributes of Table 1-4(f).	4 Calendar Months	Verify: <ul style="list-style-type: none"> • Station dc supply voltage Inspect: <ul style="list-style-type: none"> • Electrolyte level • For unintentional grounds
	18 Calendar Months	Verify: <ul style="list-style-type: none"> • Float voltage of battery charger • Battery continuity • Battery terminal connection resistance • Battery intercell or unit-to-unit connection resistance Inspect: <ul style="list-style-type: none"> • Cell condition of all individual battery cells. • Physical condition of battery rack

Table 1-4(c)

Component Type – Protection System Station dc Supply Using Nickel-Cadmium (NiCad) Batteries

Excluding distributed UFLS and distributed UVLS (see Table 3)

Protection System Station dc supply used only for non-BES interrupting devices for RAS, non-distributed UFLS system, or non-distributed UVLS systems is excluded (see Table 1-4(e)).

Component Attributes	Maximum Maintenance Interval	Maintenance Activities
	6 Calendar Years	Verify that the station battery can perform as manufactured by conducting a performance or modified performance capacity test of the entire battery bank.

<p>Table 1-4(d)</p> <p>Component Type – Protection System Station dc Supply Using Non Battery Based Energy Storage</p> <p>Excluding distributed UFLS and distributed UVLS (see Table 3)</p> <p>Protection System Station dc supply used only for non-BES interrupting devices for RAS, non-distributed UFLS system, or non-distributed UVLS systems is excluded (see Table 1-4(e)).</p>		
Component Attributes	Maximum Maintenance Interval	Maintenance Activities
Any Protection System station dc supply not using a battery and not having monitoring attributes of Table 1-4(f).	4 Calendar Months	Verify: <ul style="list-style-type: none"> • Station dc supply voltage Inspect: <ul style="list-style-type: none"> • For unintentional grounds
	18 Calendar Months	Inspect: <ul style="list-style-type: none"> • Condition of non-battery based dc supply
	6 Calendar Years	Verify that the dc supply can perform as manufactured when ac power is not present.

Table 1-4(e)		
Component Type – Protection System Station dc Supply for non-BES Interrupting Devices for RAS, non-distributed UFLS, and non-distributed UVLS systems		
Component Attributes	Maximum Maintenance Interval	Maintenance Activities
Any Protection System dc supply used for tripping only non-BES interrupting devices as part of a RAS, non-distributed UFLS, or non-distributed UVLS system and not having monitoring attributes of Table 1-4(f).	When control circuits are verified (See Table 1-5)	Verify Station dc supply voltage.

Table 1-4(f) Exclusions for Protection System Station dc Supply Monitoring Devices and Systems		
Component Attributes	Maximum Maintenance Interval	Maintenance Activities
Any station dc supply with high and low voltage monitoring and alarming of the battery charger voltage to detect charger overvoltage and charger failure (See Table 2).	No periodic maintenance specified	No periodic verification of station dc supply voltage is required.
Any battery based station dc supply with electrolyte level monitoring and alarming in every cell (See Table 2).		No periodic inspection of the electrolyte level for each cell is required.
Any station dc supply with unintentional dc ground monitoring and alarming (See Table 2).		No periodic inspection of unintentional dc grounds is required.
Any station dc supply with charger float voltage monitoring and alarming to ensure correct float voltage is being applied on the station dc supply (See Table 2).		No periodic verification of float voltage of battery charger is required.
Any battery based station dc supply with monitoring and alarming of battery string continuity (See Table 2).		No periodic verification of the battery continuity is required.
Any battery based station dc supply with monitoring and alarming of the intercell and/or terminal connection detail resistance of the entire battery (See Table 2).		No periodic verification of the intercell and terminal connection resistance is required.
Any Valve Regulated Lead-Acid (VRLA) or Vented Lead-Acid (VLA) station battery with internal ohmic value or float current monitoring and alarming, and evaluating present values relative to baseline internal ohmic values for every cell/unit (See Table 2).		No periodic evaluation relative to baseline of battery cell/unit measurements indicative of battery performance is required to verify the station battery can perform as manufactured.
Any Valve Regulated Lead-Acid (VRLA) or Vented Lead-Acid (VLA) station battery with monitoring and alarming of each cell/unit internal ohmic value (See Table 2).		No periodic inspection of the condition of all individual units by measuring battery cell/unit internal ohmic values of a station VRLA or Vented Lead-Acid (VLA) battery is required.

Table 1-5 Component Type - Control Circuitry Associated With Protective Functions Excluding distributed UFLS and distributed UVLS (see Table 3), Automatic Reclosing (see Table 4), and Sudden Pressure Relaying (see Table 5) Note: Table requirements apply to all Control Circuitry Components of Protection Systems, and RAS except as noted.		
Component Attributes	Maximum Maintenance Interval	Maintenance Activities
Trip coils or actuators of circuit breakers, interrupting devices, or mitigating devices (regardless of any monitoring of the control circuitry).	6 Calendar Years	Verify that each trip coil is able to operate the circuit breaker, interrupting device, or mitigating device.
Electromechanical lockout devices which are directly in a trip path from the protective relay to the interrupting device trip coil (regardless of any monitoring of the control circuitry).	6 Calendar Years	Verify electrical operation of electromechanical lockout devices.
Unmonitored control circuitry associated with RAS. (See Table 4-2(b) for RAS which include Automatic Reclosing.)	12 Calendar Years	Verify all paths of the control circuits essential for proper operation of the RAS.
Unmonitored control circuitry associated with protective functions inclusive of all auxiliary relays.	12 Calendar Years	Verify all paths of the trip circuits inclusive of all auxiliary relays through the trip coil(s) of the circuit breakers or other interrupting devices.
Control circuitry associated with protective functions and/or RAS whose integrity is monitored and alarmed (See Table 2).	No periodic maintenance specified	None.

Table 2 – Alarming Paths and Monitoring In Tables 1-1 through 1-5, Table 3, Tables 4-1 through 4-3, and Table 5 alarm attributes used to justify extended maximum maintenance intervals and/or reduced maintenance activities are subject to the following maintenance requirements		
Component Attributes	Maximum Maintenance Interval	Maintenance Activities
<p>Any alarm path through which alarms in Tables 1-1 through 1-5, Table 3, Tables 4-1 through 4-3, and Table 5 are conveyed from the alarm origin to the location where corrective action can be initiated, and not having all the attributes of the “Alarm Path with monitoring” category below.</p> <p>Alarms are reported within 24 hours of detection to a location where corrective action can be initiated.</p>	12 Calendar Years	Verify that the alarm path conveys alarm signals to a location where corrective action can be initiated.
<p>Alarm Path with monitoring:</p> <p>The location where corrective action is taken receives an alarm within 24 hours for failure of any portion of the alarming path from the alarm origin to the location where corrective action can be initiated.</p>	No periodic maintenance specified	None.

Table 3 Maintenance Activities and Intervals for distributed UFLS and distributed UVLS Systems		
Component Attributes	Maximum Maintenance Interval	Maintenance Activities
Any unmonitored protective relay not having all the monitoring attributes of a category below.	6 Calendar Years	<p>Verify that settings are as specified.</p> <p>For non-microprocessor relays:</p> <ul style="list-style-type: none"> • Test and, if necessary calibrate. <p>For microprocessor relays:</p> <ul style="list-style-type: none"> • Verify operation of the relay inputs and outputs that are essential to proper functioning of the Protection System. • Verify acceptable measurement of power system input values.
<p>Monitored microprocessor protective relay with the following:</p> <ul style="list-style-type: none"> • Internal self-diagnosis and alarming (See Table 2). • Voltage and/or current waveform sampling three or more times per power cycle, and conversion of samples to numeric values for measurement calculations by microprocessor electronics. <p>Alarming for power supply failure (See Table 2).</p>	12 Calendar Years	<p>Verify:</p> <ul style="list-style-type: none"> • Settings are as specified. • Operation of the relay inputs and outputs that are essential to proper functioning of the Protection System. • Acceptable measurement of power system input values.
<p>Monitored microprocessor protective relay with preceding row attributes and the following:</p> <ul style="list-style-type: none"> • AC measurements are continuously verified by comparison to an independent ac measurement source, with alarming for excessive error (See Table 2). 	12 Calendar Years	<p>Verify only the unmonitored relay inputs and outputs that are essential to proper functioning of the Protection System.</p>

Table 3 Maintenance Activities and Intervals for distributed UFLS and distributed UVLS Systems		
Component Attributes	Maximum Maintenance Interval	Maintenance Activities
<ul style="list-style-type: none"> Some or all binary or status inputs and control outputs are monitored by a process that continuously demonstrates ability to perform as designed, with alarming for failure (See Table 2). Alarming for change of settings (See Table 2).		
Voltage and/or current sensing devices associated with UFLS or UVLS systems.	12 Calendar Years	Verify that current and/or voltage signal values are provided to the protective relays.
Protection System dc supply for tripping non-BES interrupting devices used only for a UFLS or UVLS system.	12 Calendar Years	Verify Protection System dc supply voltage.
Control circuitry between the UFLS or UVLS relays and electromechanical lockout and/or tripping auxiliary devices (excludes non-BES interrupting device trip coils).	12 Calendar Years	Verify the path from the relay to the lockout and/or tripping auxiliary relay (including essential supervisory logic).
Electromechanical lockout and/or tripping auxiliary devices associated only with UFLS or UVLS systems (excludes non-BES interrupting device trip coils).	12 Calendar Years	Verify electrical operation of electromechanical lockout and/or tripping auxiliary devices.
Control circuitry between the electromechanical lockout and/or tripping auxiliary devices and the non-BES interrupting devices in UFLS or UVLS systems, or between UFLS or UVLS relays (with no interposing electromechanical lockout or auxiliary device) and the non-BES interrupting devices (excludes non-BES interrupting device trip coils).	No periodic maintenance specified	None.
Trip coils of non-BES interrupting devices in UFLS or UVLS systems.	No periodic maintenance specified	None.

<p>Table 4-1</p> <p>Maintenance Activities and Intervals for Automatic Reclosing Components</p> <p>Component Type – Reclosing and Supervisory Relay</p> <p>Note: In cases where Components of Automatic Reclosing are common to Components listed in Table 1-1 through 1-5, the Components only need to be tested once during a distinct maintenance interval.</p>		
Component Attributes	Maximum Maintenance Interval	Maintenance Activities
Any unmonitored reclosing relay or supervisory relay not having all the monitoring attributes of a category below.	6 Calendar Years	<p>Verify that settings are as specified.</p> <p>For non-microprocessor reclosing or supervisory relays:</p> <ul style="list-style-type: none"> • Test and, if necessary calibrate <p>For microprocessor reclosing or supervisory relays:</p> <ul style="list-style-type: none"> • Verify operation of the relay inputs and outputs that are essential to proper functioning of the Automatic Reclosing. <p>For microprocessor supervisory relays:</p> <ul style="list-style-type: none"> • Verify acceptable measurement of power system input values.
<ul style="list-style-type: none"> • Monitored microprocessor reclosing relay or supervisory relay with the following: Internal self-diagnosis and alarming (See Table 2). • Alarming for power supply failure (See Table 2). <p>For supervisory relay:</p> <ul style="list-style-type: none"> • Voltage waveform sampling three or more times per power cycle, and conversion of samples to numeric values for measurement calculations by microprocessor electronics. 	12 Calendar Years	<p>Verify:</p> <ul style="list-style-type: none"> • Settings are as specified. • Operation of the relay inputs and outputs that are essential to proper functioning of the Automatic Reclosing. <p>For supervisory relays:</p> <ul style="list-style-type: none"> • Verify acceptable measurement of power system input values.

Table 4-1

Maintenance Activities and Intervals for Automatic Reclosing Components

Component Type – Reclosing and Supervisory Relay

Note: In cases where Components of Automatic Reclosing are common to Components listed in Table 1-1 through 1-5, the Components only need to be tested once during a distinct maintenance interval.

Component Attributes	Maximum Maintenance Interval	Maintenance Activities
<p>Monitored microprocessor reclosing relay or supervisory relay with preceding row attributes and the following:</p> <ul style="list-style-type: none"> Some or all binary or status inputs and control outputs are monitored by a process that continuously demonstrates ability to perform as designed, with alarming for failure (See Table 2). Alarming for change of settings (See Table 2). <p>For supervisory relay:</p> <ul style="list-style-type: none"> Ac measurements are continuously verified by comparison to an independent ac measurement source, with alarming for excessive error (See Table 2). 	12 Calendar Years	Verify only the unmonitored relay inputs and outputs that are essential to proper functioning of the Automatic Reclosing.

Table 4-2(a)

Maintenance Activities and Intervals for Automatic Reclosing Components

Component Type – Control Circuitry Associated with Reclosing and Supervisory Relays that are NOT an Integral Part of an RAS

Note: In cases where Components of Automatic Reclosing are common to Components listed in Table 1-5, the Components only need to be tested once during a distinct maintenance interval.

Component Attributes	Maximum Maintenance Interval	Maintenance Activities
Unmonitored Control circuitry associated with Automatic Reclosing that is not an integral part of an RAS.	12 Calendar Years	Verify that Automatic Reclosing, upon initiation, does not issue a premature closing command to the close circuitry.
Control circuitry associated with Automatic Reclosing that is not part of an RAS and is monitored and alarmed for conditions that would result in a premature closing command. (See Table 2)	No periodic maintenance specified	None.

Table 4-2(b)

Maintenance Activities and Intervals for Automatic Reclosing Components

Component Type – Control Circuitry Associated with Reclosing and Supervisory Relays that ARE an Integral Part of an RAS

Note: In cases where Components of Automatic Reclosing are common to Components listed in Table 1-5, the Components only need to be tested once during a distinct maintenance interval.

Component Attributes	Maximum Maintenance Interval	Maintenance Activities
Close coils or actuators of circuit breakers or similar devices that are used in conjunction with Automatic Reclosing as part of an RAS (regardless of any monitoring of the control circuitry).	6 Calendar Years	Verify that each close coil or actuator is able to operate the circuit breaker or mitigating device.
Unmonitored close control circuitry associated with Automatic Reclosing used as an integral part of an RAS.	12 Calendar Years	Verify all paths of the control circuits associated with Automatic Reclosing that are essential for proper operation of the RAS.
Control circuitry associated with Automatic Reclosing that is an integral part of an RAS whose integrity is monitored and alarmed. (See Table 2)	No periodic maintenance specified	None.

Table 4-3 Maintenance Activities and Intervals for Automatic Reclosing Components Component Type – Voltage Sensing Devices Associated with Supervisory Relays Note: In cases where Components of Automatic Reclosing are common to Components listed in Table 1-3, the Components only need to be tested once during a distinct maintenance interval.		
Component Attributes	Maximum Maintenance Interval	Maintenance Activities
Any voltage sensing devices not having monitoring attributes of the category below.	12 Calendar Years	Verify that voltage signal values are provided to the supervisory relays.
Voltage sensing devices that are connected to microprocessor supervisory relays with ac measurements that are continuously verified by comparison of sensing input value, as measured by the microprocessor relay, to an independent ac measurement source, with alarming for unacceptable error or failure. (See Table 2)	No periodic maintenance specified	None.

Table 5 Maintenance Activities and Intervals for Sudden Pressure Relaying Note: In cases where Components of Sudden Pressure Relaying are common to Components listed in Table 1-5, the Components only need to be tested once during a distinct maintenance interval.		
Component Attributes	Maximum Maintenance Interval	Maintenance Activities
Any fault pressure relay.	6 Calendar Years	Verify the pressure or flow sensing mechanism is operable.
Electromechanical lockout devices which are directly in a trip path from the fault pressure relay to the interrupting device trip coil (regardless of any monitoring of the control circuitry).	6 Calendar Years	Verify electrical operation of electromechanical lockout devices.
Unmonitored control circuitry associated with Sudden Pressure Relaying.	12 Calendar Years	Verify all paths of the trip circuits inclusive of all auxiliary relays through the trip coil(s) of the circuit breakers or other interrupting devices.
Control circuitry associated with Sudden Pressure Relaying whose integrity is monitored and alarmed (See Table 2).	No periodic maintenance specified	None.



Call to Action FAC-008 Facility Ratings and Themes Report

Scott Nied
Vice President Compliance
November 9, 2022



Importance of Facility Ratings

The crux of developing accurate System Operating Limits
Without accurate ratings...

- Real-time situational awareness is impacted
 - Interface MW Flow
 - Transient Stability
 - Voltage Stability
 - System Voltage Limits
 - Interconnection Reliability Operating Limits
- System Operator response during contingencies could make things worse
- Planning studies are inaccurate
- Protection system and relay loadability settings are impacted
- Equipment is damaged





Facility Ratings are Foundational

- Interdependencies from the previous slide
- Evolving and Transforming Grid
 - Perpetual tendency to drift
 - Variable and Distributed intermittent resources; less dispatchable
 - Long term resource adequacy solutions are not known
 - Energy not always available under extreme conditions
 - FERC Order 881 – AAR coming
 - Builds confidence in the eyes of policy makers



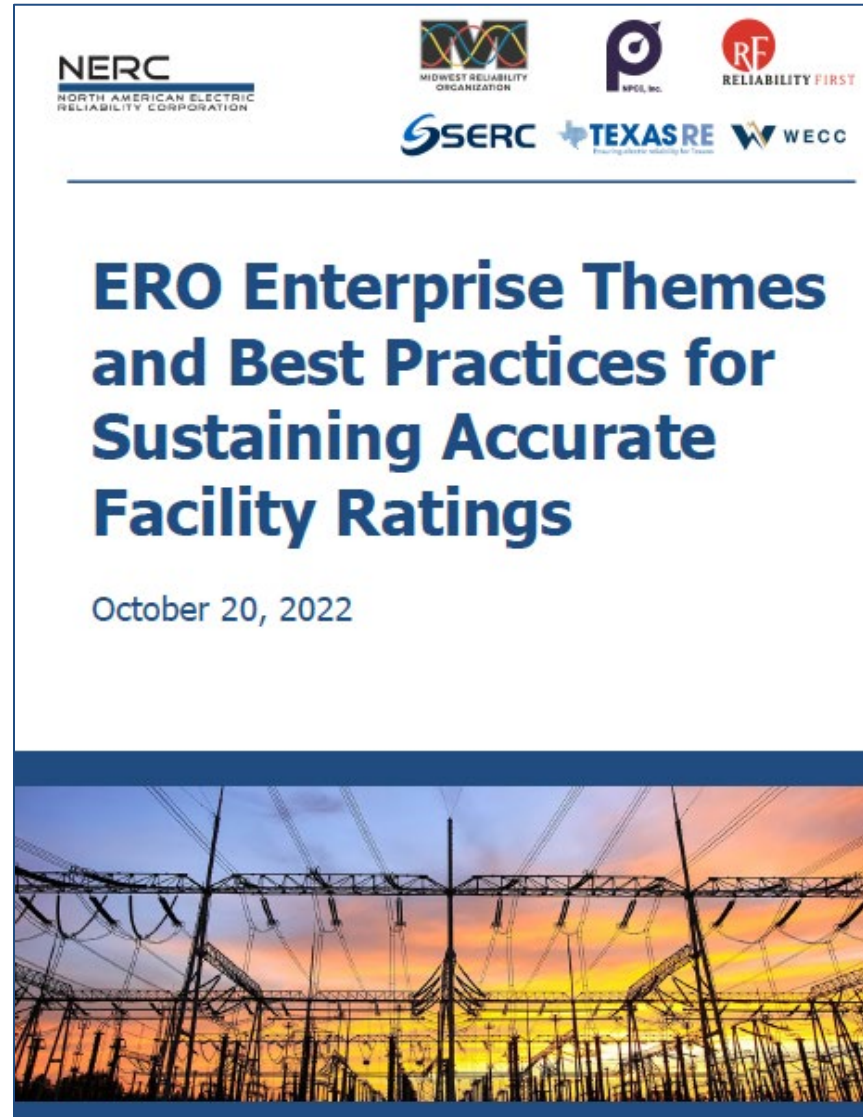
History: Focal Point of NERC and Regions

- Discussions at NERC Board of Trustees (BOT)
- FAC-008 is part of 2021/22 Risk Element in NERC Compliance Implementation Plan Training and discussions with NPCC Staff and Regional Staff
- NERC Practice Guide (published 2nd Quarter 2020)
- NERC outreach (workshops, newsletters)
- NERC External Coordination
 - NATF Facilities Ratings Practices Document (for Members)
 - FERC Focus Area during FERC observed audits
 - Facility Ratings Task Force (FRTF) under the NERC BOT



Current Status

- ERO Enterprise Facility Ratings Strategy Team
 - ERO internal extent of condition
- Strategy: Recovery Stage for 2022 - 24 via Call to Action
 - Continued communication
 - FAC-008 monitoring based on impact
 - High, Medium, Low
 - CMEP Staff Audit Approach Training
 - Mitigation Requirements
 - Touchpoints with new entities
 - Examine the current standard
- ERO Themes Report Released October 20, 2022



Best Practices



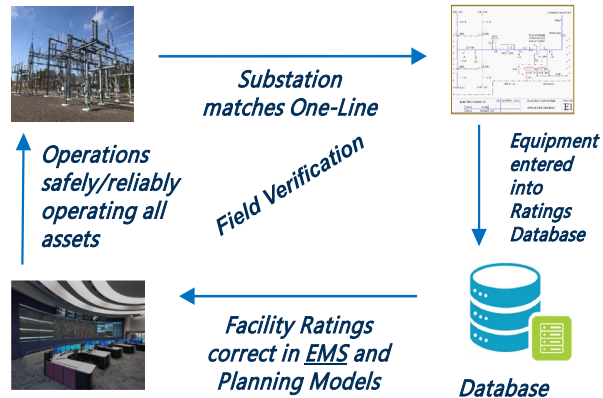
- Define Environment and Internal Controls needed to Maintain Reliable System
- Clarity on the Foundational components of the Program
- Facility Ratings Program Sponsor
- Clearly defined process, with clear roles & responsibilities
- Training for all departments and contractors involved
- Test the program; validate and verify
- Establish Accurate Baseline
- Field Verification
- Identify all Equipment – Take Photos
- Account for all necessary pieces of equipment
- Establish a Corrective Action Program – risk management and continuous improvement

Best Practices



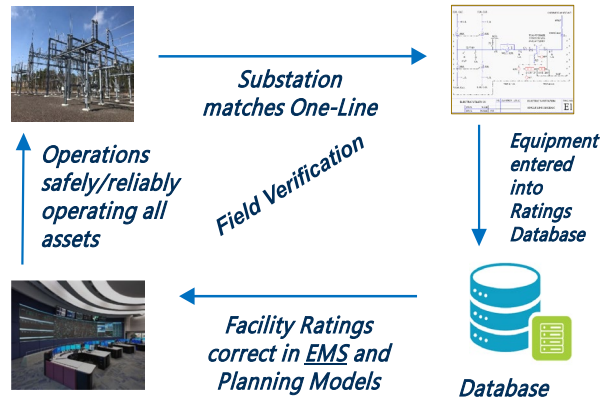
- Single Official Master Database
- Communicate location of database to all relevant personnel
- Document the process to obtain information from the field, and to enter into database
- Reinforce with Training, and workflow diagrams
- Peer review to ensure data entered correctly
- Implement strict access controls
- Contractor Management should be included

Stimulus for Errors



- Emergency Restoration
- Inventory Management
- Mergers / Acquisitions
- Database Vender Changes
- Coordination between Departments
- Equipment “removed from service”
- Changes to existing Equipment
- Commissioning of New Equipment
- Contractor work verification
- Local Office Redlines
- Underbuilds / Encroachments

Best Practices



- Change Checklist
- Quality Assurance Reviews after any change
- Validation through periodic reviews
- Data entry verification
- Periodic walk-downs
- Clearly outlined approval process
- Notification to update equipment inventory after a change is implemented
- Confirmation that change is implemented as planned
- Change process Flowchart

Best Practices



- Develop and maintain a detailed and comprehensive Facility Ratings methodology
- Use a single, consistent methodology applying the same criteria to components of a Facility
- Ensure consistent application of Facility Ratings methodology across multiple internal company divisions
- Provide the specific rating method for each class and type of element comprising a BES facility
- Train appropriate personnel on how to consistently apply the methodology
- Increase coordination with jointly-owned facilities to ensure common ratings are used

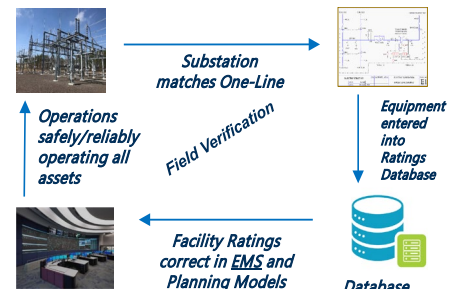
Theme 1: Lack of Awareness



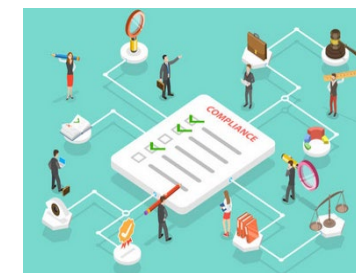
Theme 2: Inadequate Asset and Data Management



Theme 3: Inadequate Change Management



Theme 4: Inconsistent Development/ Application of Facility Rating Methodology





Aim of NPCC

- Increased entity awareness of this ERO-wide issue
- Reduce risk to the BES
 - Earlier discovery by the entity
 - Corrective and preventative mitigation starts earlier
- Adjustments to entity processes and controls result
- Entity resultant actions lend themselves to being sustainable

If you don't know where you stand, NPCC recommends:

Perform a Self-Assessment

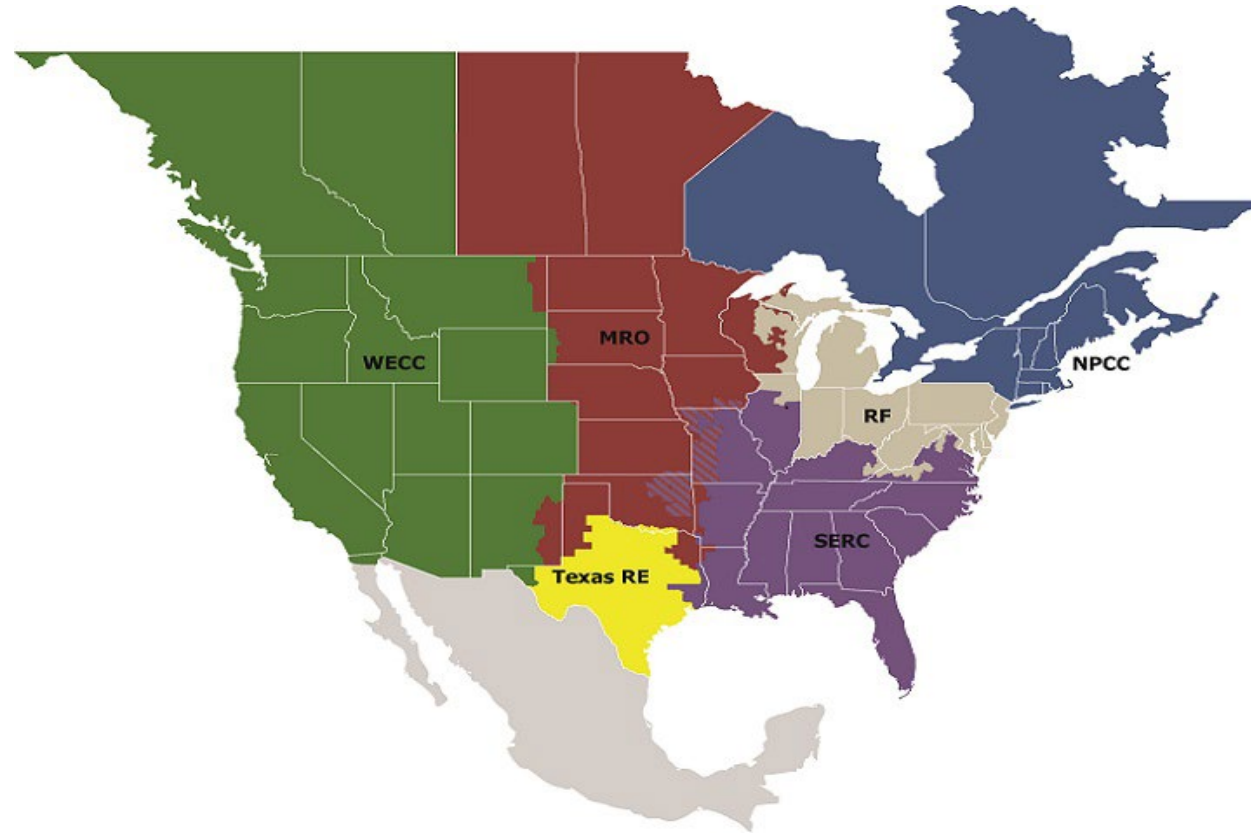
- Full vs. Partial extent of condition





Resources

- Help is available!
 - [SERC E-Learning module](#)
 - [ERO CMEP Practice Guide Facility Ratings](#)
 - [ERO CMEP Implementation Guidance FAC-008](#)
 - [RF Webinar April 4_2022 FAC_008](#)
 - [Talk With Texas May 5_2022 FAC-008](#)
- Your peers can help too
 - Find like-sized entities with similar challenges
 - What controls do they have?



Thank you for the opportunity and your time!

snied@npcc.org







Themes of Root Causes

Lack of Commitment

- Senior Management Engagement and Oversight
- An accurate baseline was never established
- Formalize training and refresh expectations
- Follow an official Corrective Action Program when issues are found

Inadequate Asset and Data Management

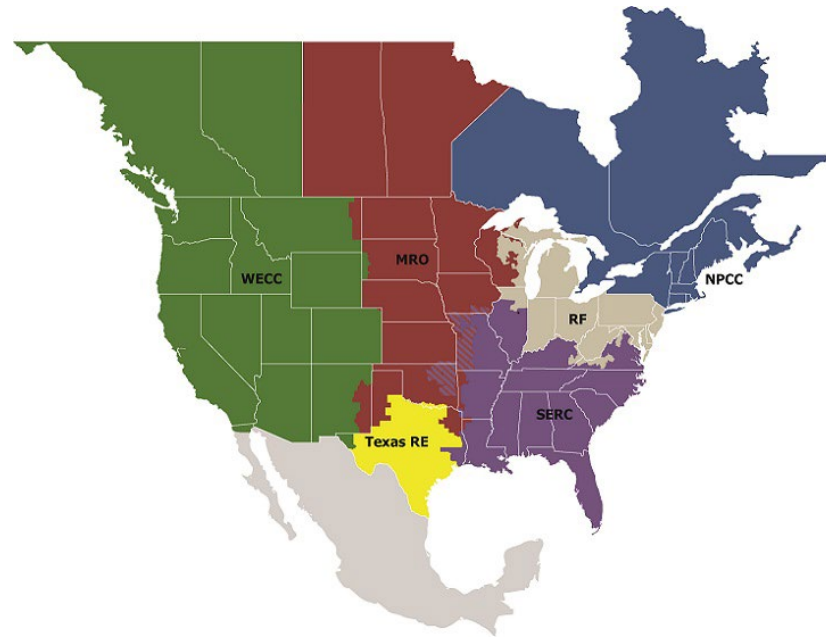
- Managing a large amount of components/Facilities
- Lack of facility ratings database with effective data capture and verification and access controls
- Reliance on contractors – oversight and commissioning

Inadequate Change Management Practices

- Establishing and maintaining strong process for communicating change amongst departments
- As-built matches design which matches EMS
- Weak data entry protocols



Aim of NPCC





Best Practices – Robust Programs Include

- A methodology that is annually reviewed with clear instructions and defined roles and responsibilities and obligations by department
- Establishment of an accurate baseline of ratings and equipment
- A mature data management process to ensure continued accuracy
- Annual training for Staff of all involved departments
- Proposed and actual changes are reviewed by Subject Matter Experts
- Required pre-change approvals and notifications
- Periodic reviews/comparisons with internal and external models
- Periodic reviews with others (e.g., construction/maintenance crews, protection and control, Control Center Energy Management System support, coordination with Reliability Coordinator and Transmission Operator, coordination of rating with the neighboring system)
- Process for ad-hoc review for unplanned or if a major event has occurred



Best Practices – Tool and Actions

- Ensure that inventory tools allow write access that is dictated by defined roles in the facility ratings methodology
- Establish automated notifications to affected groups of Facility Ratings changes
 - Protection Engineering
 - Transmission Planning
 - System Operations
 - EMS Support Team
- Validate through periodic field verification of ratings or annually – percentage/quantity determination can be based on legacy, post-event review, and new installations
- Develop a checklist for equipment changes that include:
 - Data provision obligations (internally and externally)
 - Require the need to review impacts to SOLs, protection system settings, EMS/GMS alarming impacts
- Develop a complete Facility Rating database that include all series elements and identifies the most-limiting series element(s) and includes jointly owned Facilities



Have been a focus for several years

- April 2021: Recent civil penalty in USA of \$42 million
- Issues do not appear to be declining
- What are we seeing in the field?



What have we seen? Rubber on the road examples

Missing components

- Part and pieces and parts that make up the Facility
 - Jumpers and risers inside substations, or possibly a wavetrapp
- Missing the identification of Most Limiting Series component

Incorrect ratings on components

- Current Transformers Thermal
- Jumpers/Risers Inside Substations
- Relay Thermal
- Transmission Line Conductor
- Incorrect Aluminum Conductor Stranding
- Disconnect switches

Nuances between Normal, LTE, and STE

Lack of or nonexistent coordination between neighbor TO's



NPCC Align Update

Kimberly Griffith

Senior Compliance Engineer

Daniel Kidney

Senior Compliance Engineer

Emily Stuetzle, CISA

Senior CIP Analyst

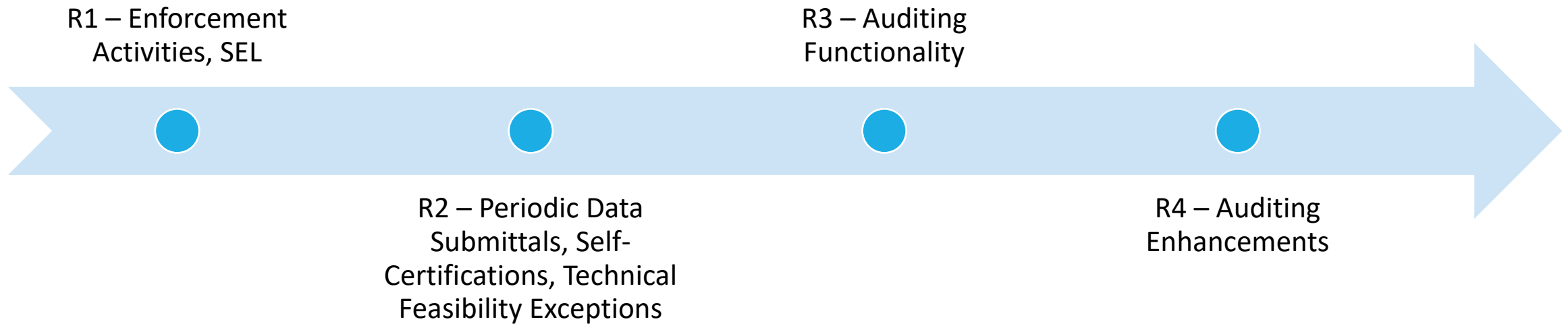
Cecil Elie, CSAP

Senior CIP Analyst





Brief Align Background and Where We Are Today



Training Opportunities



Periodic Data Submittals – Lessons Learned

Beginning with Q1 2022 FAC-003 PDS responses, new PDS response process was implemented.

This resolved an issue where only particular users were able to respond to the PDS request.

Under new process, anyone with permissions to respond to PDS (usually PCC) can open the PDS request and assign the response to any of the entity's users.

PDF instructions were sent with the Q1, Q2, Q3 PDS emails, and will be attached to future PDS request emails.



Periodic Data Submittals – 2023 Schedule

- 2023 schedule for Periodic Data Submittals can be found in the NERC One-Stop Shop ([NERC One Stop Shop](#))
 - Compliance drop down menu -> Compliance drop down menu -> 2023 ERO Enterprise Periodic Data Submittal Schedule

One-Stop-Shop (CMEP, Compliance, and Enforcement) - Active			
Documents	Year	Category	Date
Compliance (37)			
CIP ERT & User Guide (3)			
CIP FAQs (1)			
Compliance (10)			
2022 ERO Enterprise Periodic Data Submittal Schedule	2022	Compliance	12/16/2021
2023 ERO Enterprise Periodic Data Submittal Schedule	2023	Compliance	10/14/2022
CIP-008 Reliability Study Summary	2022	Compliance	8/8/2022
Compliance Webinars		Compliance	
Currently Compliant: Episode 1	2021	Compliance	2/23/2021
ERO Enterprise Compliance Auditor Checklist v6	2022	Compliance	3/24/2022
ERO Enterprise Compliance Monitoring and Enforcement Manual v6	2022	Compliance	3/24/2022
Regional Audit Reports of Registered Entities		Compliance	
Reliability Standard Audit Worksheets (RSAWs)		Compliance	
Sampling Lead Sheet Template		Compliance	



Periodic Data Submittals – 2023 Schedule

Includes due dates for all standards that have Periodic Data Submittals requirements.

FAC-003 Vegetation quarterly due dates – 20 days after end of each quarter

- Q4 2022 – January 20, 2023
- Q1 2023 – April 20, 2023
- Q2 2023 – July 20, 2023
- Q3 2023 – October 20, 2023
- Q4 2023 – January 20, 2024



Periodic Data Submittals – Attestation Renewals

FAC-003 Vegetation applicability can be found in sections 4.2 and 4.3 for Transmission Owners and Generator Owners respectively.

Entities registered for those functions for which FAC-003 is not applicable have the option to submit an attestation in lieu of quarterly PDS responses.

Attestations valid for one year – FAC-003 PDS requests are not submitted to entities with an active, valid attestation.

Attestations that were submitted during 2022 will require reaffirmation in 2023.

NPCC will request reaffirmation when renewal date is approaching.



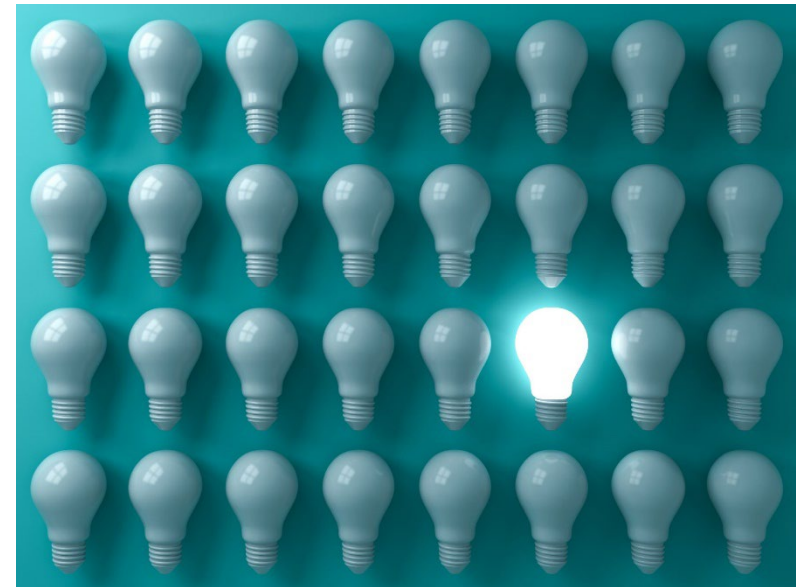
Self-Certifications In Align – Lessons Learned

RFIs

- Each RFI will have its own SEL Ref ID
- Only person who entered an RFI can mark it complete – Request for Enhancement

Close-out Notes

- Results
- Summary Letter





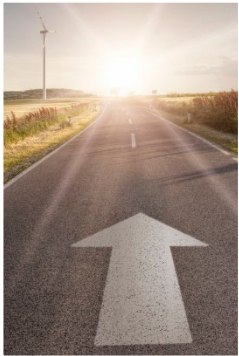
Auditing in Align - Lessons Learned



- **Failure to utilize the appropriate SEL Reference ID for uploading evidence can result in extended auditor review time prolonging the completion of the audit and re-submission of data utilizing appropriate SEL Reference IDs.**
- Multiple evidence files may be uploaded at one time.
(Associated SEL Reference ID & Align RFI number)
- **Challenge for 1st audit pilot: access to Align platform**
Advise compliance engagement team lead
Support Process



Where We're going in the Future



Continued Align Pilots into 2023



R4.5 – IRAs and COPs

- Soft Go-Live Q4 2022
- Training to be offered late Q4 2022 and/or early Q1 2023
- Pilot Entities



Continued Helpdesk Support and Training Opportunities



Improvements to existing functionality



Resources

NPCCAlignTeam@npcc.org

NERC Training Videos and User Guides

<https://support.nerc.net>

NPCC's Align Quick Reference Guide

Recorded Training Sessions

SEL Data Handling Guidance and Align Oversight Industry [Webinar](#) (December 5, 1PM EST)



NORTH

COORDINATING COUNCIL, INC.



Questions

Kimberly Griffith
kgriffith@npcc.org

Daniel Kidney
dakidney@npcc.org

Emily Stuetzle, CISA
estuetzle@npcc.org

Cecil Elie, CSAP
celie@npcc.org

PUBLIC

NPCC Compliance Oversight Plan (COP) Enhancements and Status

Ben Eng
NPCC
Manager, Entity Risk Assessment
*'Assuring BES Reliability through
Risk and Controls Management'*



CMEP Process Overview



Compliance Oversight Plan

The COP is an entity-specific report consisting of entity-specific risks identified through analysis of both Inherent Risk Assessment (IRA) and Performance Considerations¹.

- Provides an oversight strategy with a target interval and frequency for oversight activities.
- Tailored to each entity's entity specific risks based on inherent and operational risks (the IRA, Performance Considerations), and associated Risk Categories.
- Is dynamic and requires change management to capture changes that may impact Reliability and Risks.



Enhanced Analysis

Inherent & Performance Data

Analysis of inherent and performance data provides an understanding of an entity's overall inherent risk and performance

¹²profile



Targeted Oversight

Risk Categories

Selected risks provide a focus for an entity's continuous improvement & to Regional Entities for its compliance monitoring activities



Prioritized Monitoring

Oversight Strategies

Provide target interval frequency for oversight, primary monitoring tools, and informs annual planning



Standards to Risk

Appendix B

Provides Reliability Standards associated with the entity-specific risks. The scope of monitoring activities is derived from this list



COP Report

Common Template

One report to provide both inherent risk assessment results and the compliance oversight plan

Enhancement #1

- Create more COPs
- Get them into the hands of the entities sooner so that they can be used as a strategic planning tool in advance of scheduled monitoring.

Enhancement #2

- ERA staff has recently doubled/tripled



**Matthew A.
Forrest**

Senior O&P Entity
Risk Analyst



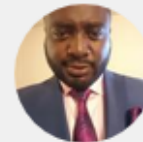
**Thomas E.
Buhler**

Senior Entity Risk
Assessment
Analyst



**Brian J.
Robinson**

Senior Entity Risk
Assessment
Analyst



Thierry Ngassa

Senior O&P Entity
Risk Assessment
Analyst

- ERA 2023 Work Plan to implement Enhancement #1, and ensuing enhancements

COP Enhancement #3

- Provide better correlation between Audit Notification Letter/Scope and COP
- Will include Focus Areas in COP Appendix B to add value as a strategic planning tool.
- NERC/NPCC 2023 Focus Areas will be posted on NPCC website.
 - Added transparency to entities who have not received COPs.
 - CMEP IP continues the practice of not requiring Regional Entities to post Implementation Plans.

COP Enhancement #4

- After an audit, update the COP in a reasonable timeframe
- The entity can acquire and use the feedback to focus on areas for improvement until the next engagement is scheduled
- The update takes into account the audit results, performance considerations, and other entity specific inputs that help refine the standards subject to monitoring, monitoring method and interval.

COP Enhancement #5

Performance Considerations (PCs) – progress continues

- *Affiliates* removed as a Performance Consideration.
- Getting close to determining metrics for Misoperations (MIDAS), Transmission Availability (TADS), Generation Availability (GADS), Events (TEAMS). Discussions continue between NERC RAPA group and RAPTF.
- Internal Controls (once considered a primary performance consideration) is now a secondary performance consideration to refine monitoring.
 - ICTF developed ICAT template to document and assess entity controls to mitigate risks in Risk Categories.
 - ICTF discussing use of Maturity Model to evaluate entity Enterprise level internal controls.
- Compliance History and Culture of Compliance remain same.

COP Ongoing Issues

- COP *Oversight Category* language – “without demonstrated positive performance”
- Metrics to support *Oversight Category* “with Demonstrated Positive Performance”
- Coordination with Align version 4.5 development team.

Questions?

- My name is Ben Eng
- I can be reached at beng@npcc.org
or the ERA group at era@npcc.org
- Thank you for your attention!



NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Compliance Guidance

Kiel Lyons, Senior Manager, Compliance Assurance
November 9, 2022

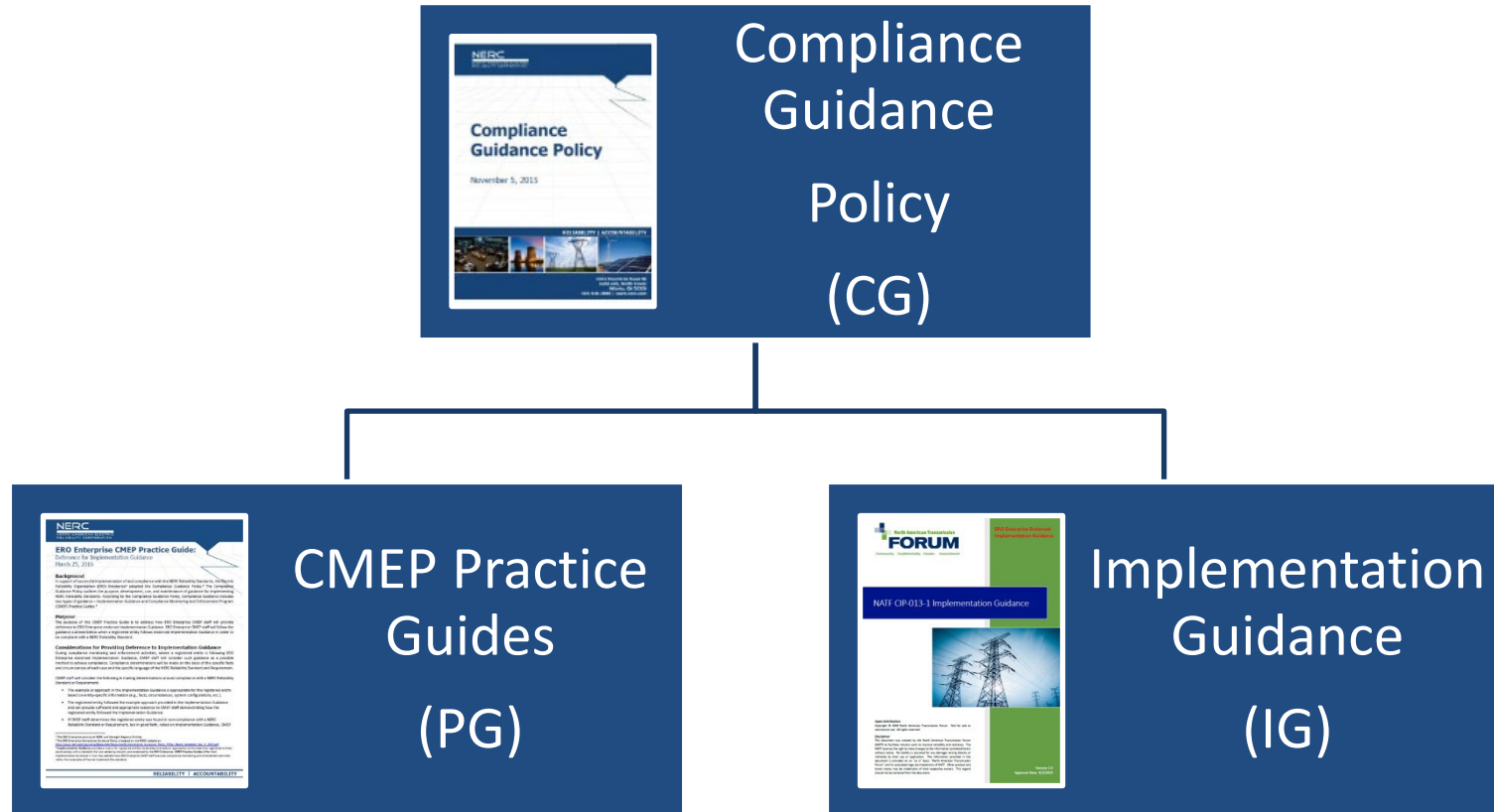
RELIABILITY | RESILIENCE | SECURITY



- Compliance Guidance Policy
- CMEP Practice Guides
- Implementation Guidance
- Program Evolution
- Tools & Resources

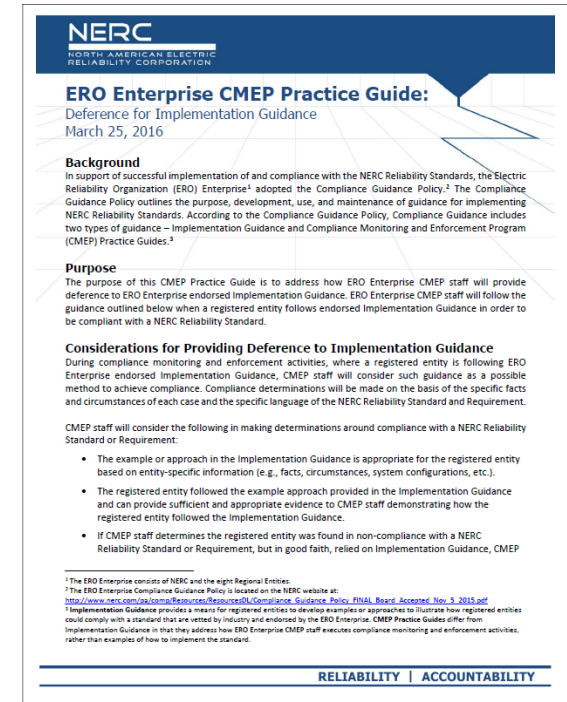
- Multiple Guidance Documents
 - CANs, CARs, Directives, Bulletins, etc.
- Desire to Consolidate Guidance
 - Reduce Confusion
- Compliance Guidance Review Team
 - Recommendation to NERC BOT
 - Finite/Limited Guidance Tools
- NERC BOT Approved CG Policy
- Supporting Tools and Resources Developed





- **CMEP Practice Guides (PG)**

- How CMEP Personnel Execute CMEP Activities
- Reliability Standard or Topic Specific
- Developed by ERO Enterprise for ERO Enterprise
- Development Process
 - Need Identified
 - Industry or ERO Enterprise Feedback
 - Development
 - ERO Enterprise Technical Task Forces
 - CCC Review: Comments Considered
 - Approval
 - ERO Enterprise CMEP Management
- Publically Posted for Transparency



- **Implementation Guidance (IG)**
 - Examples or Approaches
 - Industry “Implement” Reliability Standards
 - Developed by Industry for Industry
 - Pre-Qualified Organization (PQO)
 - Standard Drafting Team (SDT)
 - Regional Entity Stakeholder Committees
 - Does Not Guarantee Compliance
 - Not only way to comply
 - Facts, Circumstances, and Configurations
 - Industry Vetted
 - Endorsed by ERO Enterprise
 - Publically Posted





- **Develop**

- Implementation Guidance Training by NERC
 - Before Work Begins
- Utilize Development Tools
 - Avoid Pitfalls
- Collaborate
 - Avoid Duplicative Work
 - Leverage Knowledge
- IG Management
 - Ensure Guidance Remains Relevant and Useful
 - Periodic Review Requirement
- Submit



- **Review**

- Received by ERO Enterprise Subject Matter Experts (SME)
- Utilize Review Tools
- Collaborate
 - Internal Regional and NERC Departments
 - Compliance, Enforcement, Risk
- Vet
 - ERO Enterprise Task Forces
 - Include NERC and Regional Representatives
 - * Operations & Planning Compliance Task Force
 - * CIP Compliance Task Force
- Recommend
 - To ERO Enterprise CMEP Management
 - One ERO Enterprise Statement
 - Non-Endorsement Recommendations Only



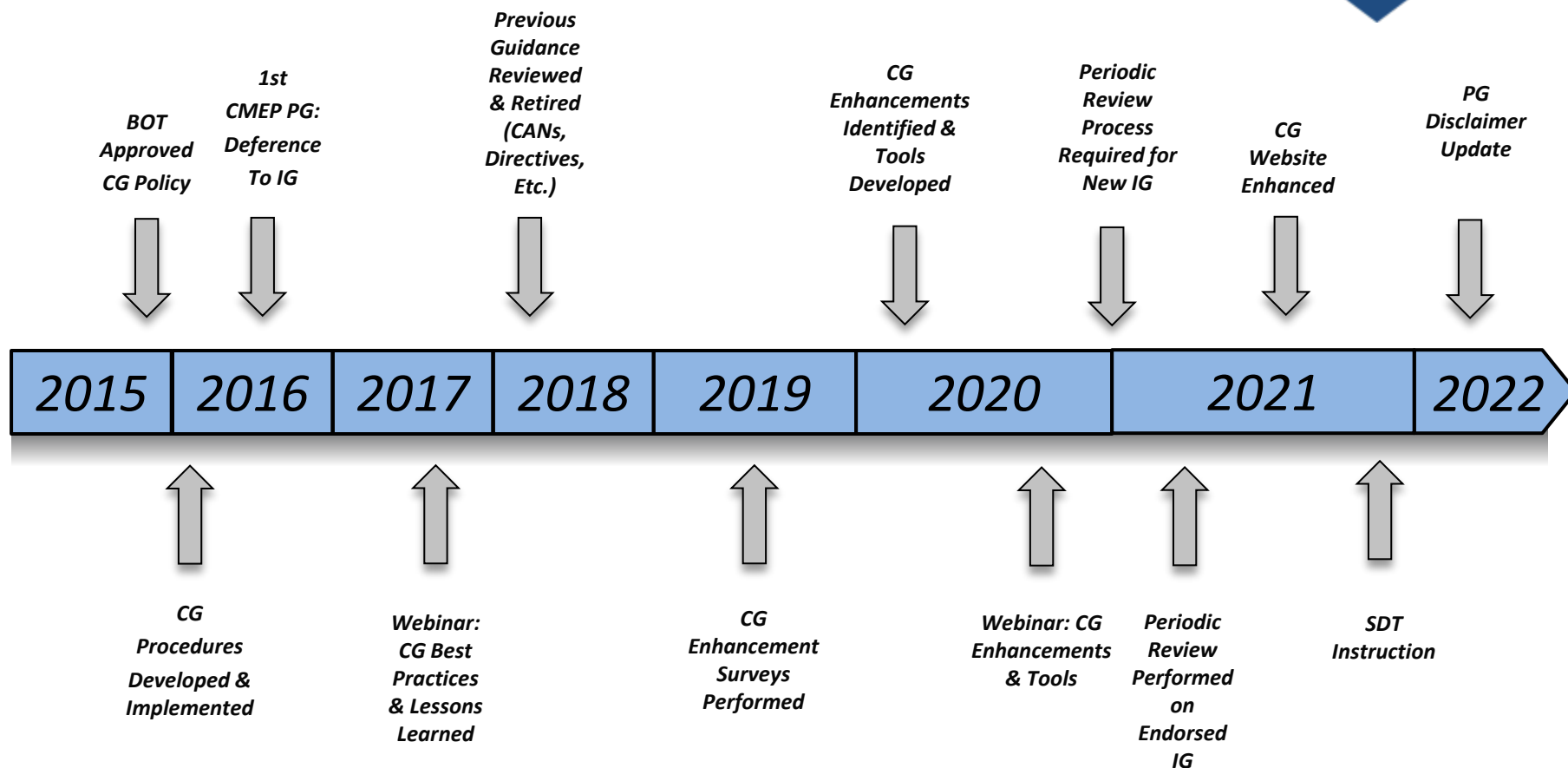
- **Endorse**

- ERO Enterprise CMEP Management
 - Receive Task Force Recommendation
 - Risk Performance Management Group (RPMG)
- Collaborate on TF Recommendation
 - Openly Discuss Identified Issues
- Endorse or Not Endorse
- Final Review
 - NERC Director of Enforcement
- Notify, Post, Announce



- **Program Evolution**

- Initial Processes & Tools Developed
- Initial Industry Outreach Performed
- Retirement of Legacy Guidance
- Enhancement Surveys Performed
 - Revised/Developed Processes & Tools
 - Industry Outreach on Processes & Tools
- Incorporated Periodic Review requirement
 - ERO Enterprise Performed Initial Periodic Review
- Enhanced Compliance Guidance Website
- IG Development
 - Offer to Provide IG 101 to New STD
 - CA Staff Observe Development of IG – Provide Recommendations
 - Encourage Early Coordination



• Tools & Resources

- IG Template*
- IG Development and Review Aid*
- Non-Endorsed IG Tracking
- IG Under Consideration/Development Spreadsheet
- PQO/SDT Contact Information
- Compliance Guidance Webpage
- One-Stop Shop (Standards and CMEP)*
- Technical Committee Sites

* Reviewed during this presentation

- **IG Template**

- Common Look and Arrangement
 - Basic Sections
 - Common Sense Flow
- PQO Logo
 - Identify Owner
 - Acknowledgment of Work

PROPOSED Implementation Guidance - NOT ERO Enterprise Endorsed

PQO
LOGO
HERE

Implementation Guidance Title
Reliability Standard and Requirement
Reliability Standard and Requirement (If Needed)

Date
DELETE AFTER READING: PQO and SDT are strongly encouraged to reference the *Implementation Guidance Development and Review Aid* [here](#) prior to developing IG documents

- **IG Template** (continued)
 - Title Page
 - Descriptive Information
 - Logos
 - Table of Contents
 - Introduction
 - Goal/Problem Statement
 - Reliability Standard
 - Requirement
 - Examples

PROPOSED Implementation Guidance - NOT ERO Enterprise Endorsed	
Table of Contents	
Introduction	3
Goal/Problem Statement	3
Scope	3
Reliability Standard	3
Requirement X	3
Example 1	3
Example 2	3
Requirement X	3
Example 1	4
Example 2	4
Periodic Review	4
Appendices	5
Appendix – Sources and Resources	5
Appendix X	5
Appendix X	5

PROPOSED Implementation Guidance - NOT ERO Enterprise Endorsed	
Introduction	
Provide a brief introduction/background statement on the purpose of the subject Reliability Standard, what aspect of the purpose does the subject Requirement(s) address, and how the Requirement(s) addresses that aspect. Example topics could include; historical perspectives, relevant FERC orders, related guidance, committees work, standard revisions, how the need for the Implementation Guidance was identified, etc.	
Goal/Problem Statement	
Provide a brief problem statement, as applicable, to identify the goal of the Implementation Guidance or the problem(s) the Implementation Guidance addresses. Problem statements could speak to reliability challenges, compliance challenges, changing technology, differing viewpoints, etc.	
Scope	
Provide a brief statement on the scope of the proposed Implementation Guidance. State what is included, and what is not included, in the scope of the proposed Implementation Guidance document. This section should include a disclaimer stating that following the Implementation Guidance does not guarantee compliance and is based on precise language of the standard, individual facts, circumstances, system configuration, quality of evidence, etc.	
Reliability Standard	
Copy and the Paste the relevant sections of the subject Reliability Standard as applicable. Example sections could include the Purpose, Applicability, Effective Date, Compliance, etc.	
Requirement X	
Copy and the Paste the subject Requirement.	
Provide a detailed description of the issues/concerns with the Requirement that the proposed IG will address.	
Example 1	
Provide detailed examples, methodologies, or approaches that an entity could follow and would generally lead to compliance with the Requirement (dependent upon individual facts, circumstances, and system configuration).	
Example 2	
Provide detailed examples, methodologies, or approaches that an entity could follow and would generally lead to compliance with the Requirement (dependent upon individual facts, circumstances, and system configuration).	
Requirement X	
Copy and the Paste the subject Requirement.	
Implementation Guidance Title	

- **IG Template** (continued)
 - Periodic Review
 - Ensures Relevance
 - Appendices
 - Supporting Information

PROPOSED Implementation Guidance - NOT ERO Enterprise Endorsed

Provide a detailed description of the issue(s)concerns with the Requirement that the proposed IG will address.

Example 1
Provide detailed examples, methodologies, or approaches that an entity could follow and would generally lead to compliance with the Requirement (dependent upon individual facts, circumstances, and system configuration).

Example 2
Provide detailed examples, methodologies, or approaches that an entity could follow and would generally lead to compliance with the Requirement (dependent upon individual facts, circumstances, and system configuration).

Periodic Review
Provide a description of the PQOs/SDTs plan to perform periodic reviews to ensure IG, if endorsed, will remain current and valid. Maintenance plans should address, at a minimum, the periodicity of the review, who will perform the review, how the review will be initiated, and what will be reviewed. Reviews should include items such as updates or revisions to items such as FERC Orders, FERC interpretations, Reliability Standard Audit Worksheets (RSAW), Endorsed Implementation Guidance, Compliance Bulletins and Directives, Reliability Standard Implementation Plans, Reliability Standard Guidelines and Technical Basis, Technical Rationale, new technology, NERC Glossary of Terms, etc.

PROPOSED Implementation Guidance - NOT ERO Enterprise Endorsed

Appendices
The appendices should be used to house information that is relevant but otherwise should not be included in the body of the Implementation Guidance. Appendices could include templates, theory, calculations, models, tables, drawings, graphics, good practices, definitions, terminology, glossary, white papers, FERC orders, Guideline and Technical Basis, Technical Rationale, IG authors, etc.

Appendix – Sources and Resources
Consider using a list of hyperlinks in the Appendices for publically available supporting/reference documents, and only include actual documents in the Appendices for non-publically available supporting/reference documents.

Appendix X

Appendix X

Implementation Guidance Title 4

Implementation Guidance Title 5

- **IG Development and Review Aid**
 - Used by Developers and Reviewers

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Implementation Guidance Development and Review Aid

October 2020

Implementation Guidance (IG) provides a means for industry¹ to develop examples or approaches to illustrate how registered entities could comply with a Standard. Examples provided in IG are not exclusive, as there are likely other methods for implementing efforts to comply with a Standard. The ERO Enterprise's endorsement² of an example means the ERO Enterprise CMEP staff will give these examples deference when conducting compliance monitoring activities. Registered entities can rely upon the example and be reasonably assured that compliance requirements will be met with the understanding that compliance determinations depend on facts, circumstances, and system configurations.

In order to ensure IG documents are beneficial to industry Pre-Qualified Organizations (PQO) and Standard Drafting Teams (SDT) should consider developing IG before it is needed by industry. Additionally, in order to reduce the amount of IG documents addressing the same or closely related issues the PQO and SDT³ should consider collaborating with other [PQO and SDT contacts](#) who may be developing similar guidance. Proactively [notifying NERC](#) of IG under development, or under consideration for development, will ensure the [IG Under Development/Consideration Tracking](#) spreadsheet remains current and useful. PQO and SDT are encouraged to utilize the [ERO Enterprise Implementation Guidance Template](#) when developing or revising Implementation Guidance.

Proposed IG should consider items in the table below to reduce risk of non-endorsement.

¹ Pre-Qualified Organizations (PQO) and Standard Drafting Teams (SDT)
² The ERO Enterprise endorses the examples and approaches only. The ERO Enterprise endorsement does not include supporting documentation or links included in IG appendices such as white papers, theory, background, history, FAQ, etc.
³ The BOT Approved Compliance Guidance Policy, Footnote 7, states "The drafting team can and should reach out to industry for assistance, as needed".

RELIABILITY | RESILIENCE | SECURITY

Color Code Key:

Automatic Non-Endorsement

Increased Likelihood of Non-Endorsement

Multiple Occurrences/Severity of Occurrences could lead to Non-Endorsement

Implementation Guidance Development Aid		
	Items for Consideration	✓
1.	Ensure IG does not conflict with, or change, the Purpose or Applicability of the Reliability Standard.	
2.	Ensure IG does not conflict with, or change, the meaning or intent of the Requirement and Measure.	
3.	Ensure IG does not include language that attempts to describe an audit approach.	
4.	Ensure IG does not conflict with, or contradict, FERC or ERO Enterprise documents such as FERC Orders, FERC Interpretations, Reliability Standard Audit Worksheets (RSAW), Endorsed Implementation Guidance, Compliance Bulletins and Directives, Reliability Standard Implementation Plans, Reliability Standard Guidelines and Technical Basis, NERC Glossary of Terms, etc.	
5.	Ensure IG does not make the Reliability Standard and Requirement less restrictive.	
6.	Ensure IG does not lead the entity to believe there are additional compliance obligations that are not specifically required by the subject Reliability Standard and Requirement.	
7.	Ensure IG does not skip steps or stop short of complying, and addresses the entire Requirement in sufficient detail.	
8.	Ensure IG provides specific examples or approaches to compliance.	
9.	Ensure IG is not a whitepaper, position paper, concept paper, FAQ, or technical reference document.	
10.	Ensure the body of the IG document only includes specific examples or approaches to compliance and does not include supporting/reference information that should be housed in the Appendices. NOTE: Appendices could include templates, theory, calculations, models, tables, drawings, graphics, good practices, definitions, terminology, glossary, white papers, FERC orders, Guideline and Technical Basis, Technical Rationale, IG authors, etc.	
11.	Ensure IG is not region specific, such as guidance for a Regional Reliability Standard.	
12.	Ensure IG includes a plan for PQO/SDT periodic reviews and updates to ensure guidance remains current and valid. Reviews should include elements such as updates or revisions to items such as FERC Orders, FERC Interpretations, Reliability Standard	

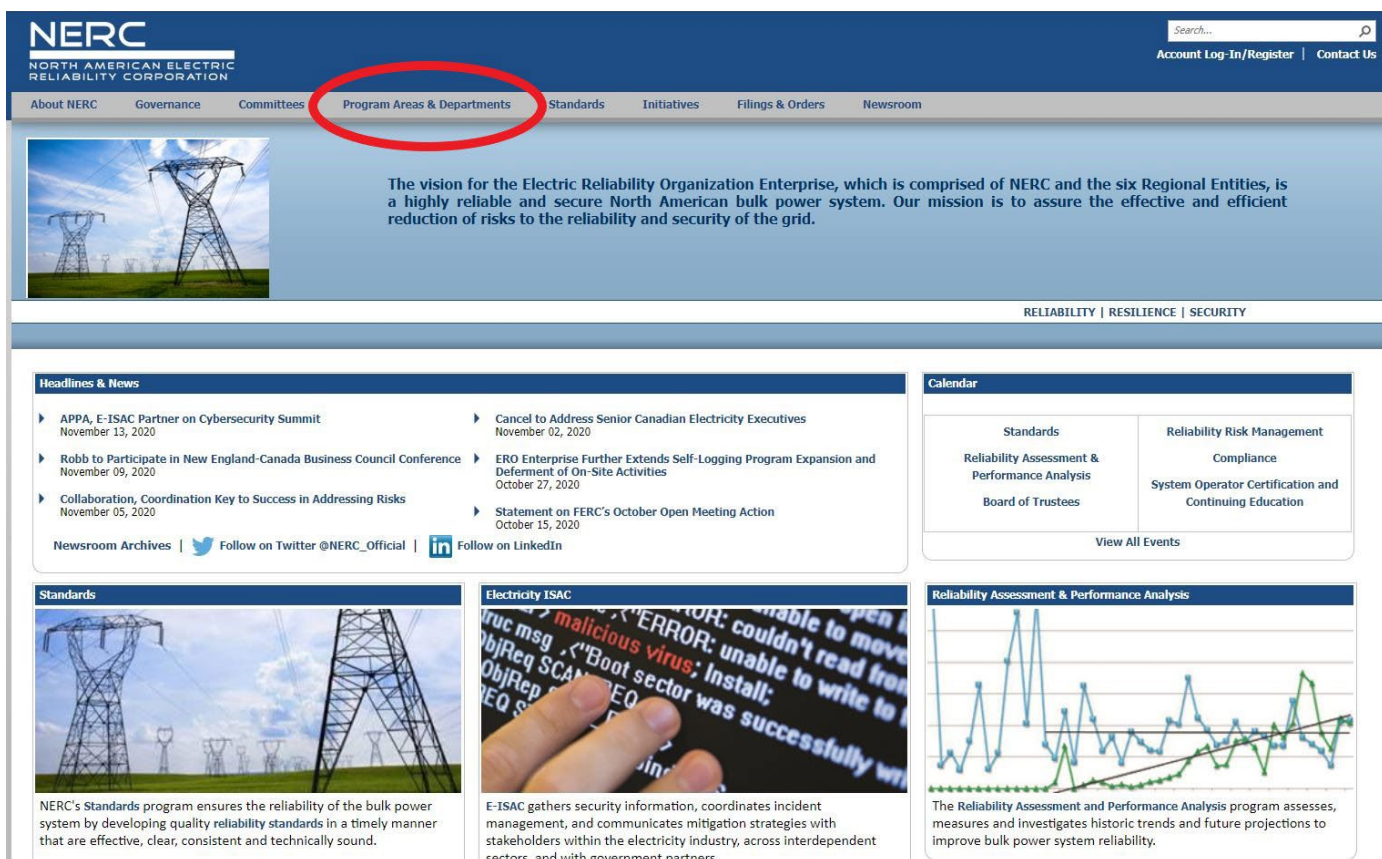
	Audit Worksheets (RSAW), ERO Endorsed IG, Compliance Bulletins and Directives, Reliability Standard Implementation Plans, Reliability Standard Guidelines and Technical Basis, Technical Rationale, new technology, NERC Glossary of Terms, etc.	
13.	Consider utilizing the ERO Enterprise Implementation Guidance Template to allow for a common look and feel, and user familiarity.	
14.	Consider if an entity followed the approach or example, would it generally lead the entity to compliance.	
15.	Ensure IG only addresses one, or very limited and closely related, Reliability Standards and Requirements to ensure it is not unnecessarily large or attempts to be all encompassing.	
16.	Consider using a list of hyperlinks in the Appendices for publically available supporting/reference documents, and only include actual documents in the Appendices for non-publically available supporting/reference documents.	
17.	Ensure specialized terminology, such as used by technical committees, is defined in the IG document and the definition does not conflict with related terminology defined in the NERC Glossary of terms.	
18.	Ensure IG capitalizes terms defined in the NERC Glossary of Terms.	
19.	Consider using softer words such as "should consider", "may want to", "recommended", etc. when the processes, procedures, or approaches described are examples and are not mandatory.	
20.	Consider using language that is clear, concise, and complete, and focuses on the quality (not quantity) of subject material.	
21.	Consider the Applicability of the subject Reliability Standard and Requirement, and if the guidance is written in a manner that is useful to all applicable registered functions.	
22.	Consider using the specific language of the subject Reliability Standard and Requirement rather than attempting to explain the criteria (i.e. the Requirement) using different verbiage, when possible.	
23.	Ensure the IG does not reference inactive Reliability Standards or use terminology that was used in previous versions of a Reliability Standard, and are no longer in use in the subject version of the subject Reliability Standard.	
24.	Ensure IG correctly references footnotes, citations, illustrations, table numbers, Attachments, Addendums, Appendices, Etc.	
25.	Consider the reliability, credibility, validity of external sources being cited. NOTE: IG should be standalone documents and should not rely on external sources.	
26.	Ensure the latest version web site links, resources, etc. is being referenced.	
27.	Consider eliminating, or limiting, the use of embedded documents if used.	
28.	Consider spelling out, or defining, acronyms during their initial use.	
29.	Consider using illustrations such as diagrams, sample records, flowcharts, templates, etc.	

30.	Consider the value of developing IG that addresses Reliability Standards and Requirements that are subject to near future retirement or revision.	
31.	Consider including a disclaimer that following the IG does not guarantee compliance.	
32.	Standard Drafting Teams (SDT) should write clear compliance expectations into the Requirements of the Reliability Standard, and not in IG (Applicable to SDT only).	
33.	Consider reaching out to NERC Compliance staff here with questions that arise during development.	
34.	Consider reaching out to NERC Compliance staff here regarding a preliminary review of proposed IG prior to formal submittal.	
35.	Consider reaching out to NERC Standards Program Contacts here with questions regarding standard revisions or development, as needed.	

- Standards One-Stop-Shop
 - Survey Results Addressed: Duplicative Guidance, IG Timeliness
 - Spreadsheet Includes Links to Related Guidance
 - Maintained by NERC Standards Department

Status	Standard Version	Board Adopted Date	Effective Date of Standard	Inactive Date	Implementation Plan	Related Documents	Public Notes	FERC Orders (Date Issued)	RSAs (Enforceable Standards Only)	Lessons Learned	Compliance Guidance
Inactive	CIP-002-5.1	9/27/2013	7/1/2016	12/26/2016	Implementation Plan		Errata approved by the SC on 9/27/2013. See also CIP V5 Effective Dates here under Key Resources: http://www.nerc.com/pa/CIP/Pages/Transition-Program.aspx	11/22/2013	BSA	CIP Version 5 Transition Program	5/20/2016, Compliance Guidance Updates
Mandatory Subject to Enforcement	CIP-002-5.1a	11/2/2016	12/27/2016		Implementation Plan	Interpretation	Interpretation of CIP-002-5.1 for Energy Sector Security Consortium (EnergySec)		BSA		2/3/2018
Filed and Pending Regulatory Approval	CIP-002-6	5/14/2020			Implementation Plan						
Inactive	CIP-003-3	12/16/2009	10/1/2010	6/30/2016	Implementation Plan			2/31/2010	BSA		
Inactive	CIP-003-3a	11/7/2013		6/30/2016	Implementation Plan				BSA		
Inactive	CIP-003-5	11/26/2012		6/30/2016	Implementation Plan			11/22/2013		CIP Version 5 Transition Program	
Inactive	CIP-003-6	2/12/2015	7/1/2016	12/31/2019	Implementation Plan		With the approval of CIP-003-7 and its associated Implementation Plan, entities will not be required to implement CIP-003-6, Requirement R2, Attachment 1, Sections 2 and 3. Instead, entities will implement CIP-003-7, Requirement R2, Attachment 1 Sections 2 and 3 on January 1, 2020. See Implementation Plan for CIP-003-7.			CIP Version 5 Transition Program	5/20/2016, Compliance Guidance Updates

- NERC Homepage (www.nerc.com)
 - Survey Results Addressed: Update Compliance Guidance Webpage



The screenshot shows the NERC homepage. The navigation bar includes links for About NERC, Governance, Committees, **Program Areas & Departments** (circled in red), Standards, Initiatives, Filings & Orders, and Newsroom. Below the navigation bar is a large banner with the text: "The vision for the Electric Reliability Organization Enterprise, which is comprised of NERC and the six Regional Entities, is a highly reliable and secure North American bulk power system. Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid." Below the banner is a section titled "Headlines & News" with several news items. To the right is a "Calendar" section with a table of events. Below the headlines is a "Standards" section with an image of power lines and text about the Standards program. To the right is an "Electricity ISAC" section with an image of a hand pointing at a screen displaying error messages. Below that is a "Reliability Assessment & Performance Analysis" section with a line graph and text about the program's purpose.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Search...

Account Log-In/Register | Contact Us

About NERC | Governance | Committees | **Program Areas & Departments** | Standards | Initiatives | Filings & Orders | Newsroom

The vision for the Electric Reliability Organization Enterprise, which is comprised of NERC and the six Regional Entities, is a highly reliable and secure North American bulk power system. Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

RELIABILITY | RESILIENCE | SECURITY

Headlines & News

- ▶ APPA, E-ISAC Partner on Cybersecurity Summit
November 13, 2020
- ▶ Robb to Participate in New England-Canada Business Council Conference
November 09, 2020
- ▶ Collaboration, Coordination Key to Success in Addressing Risks
November 05, 2020
- ▶ Cancel to Address Senior Canadian Electricity Executives
November 02, 2020
- ▶ ERO Enterprise Further Extends Self-Logging Program Expansion and Deferment of On-Site Activities
October 27, 2020
- ▶ Statement on FERC's October Open Meeting Action
October 15, 2020

Newsroom Archives | [Follow on Twitter @NERC_Official](#) | [Follow on LinkedIn](#)

Calendar

Standards	Reliability Risk Management
Reliability Assessment & Performance Analysis	Compliance
Board of Trustees	System Operator Certification and Continuing Education

[View All Events](#)

Standards

NERC's Standards program ensures the reliability of the bulk power system by developing quality reliability standards in a timely manner that are effective, clear, consistent and technically sound.

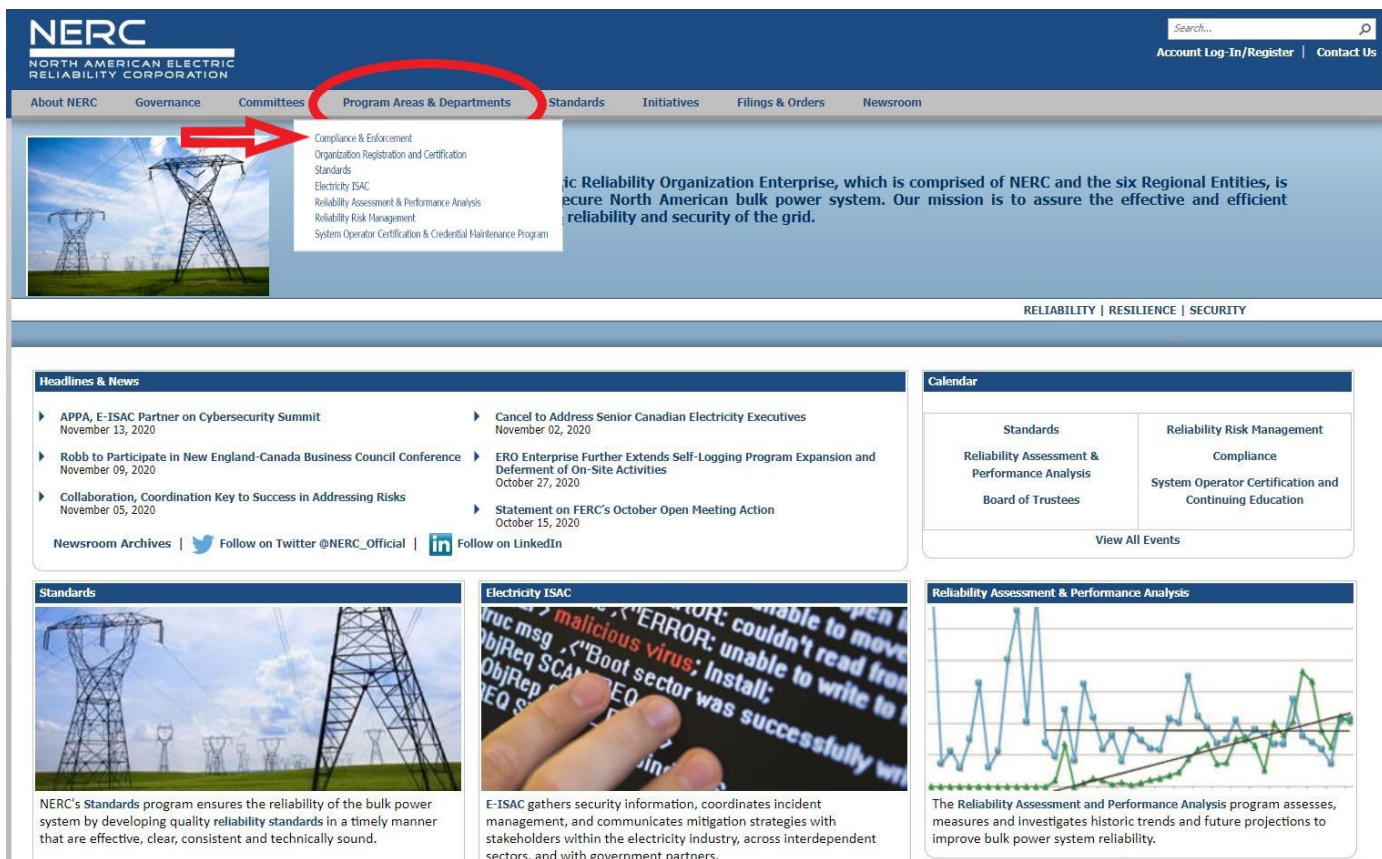
Electricity ISAC

E-ISAC gathers security information, coordinates incident management, and communicates mitigation strategies with stakeholders within the electricity industry, across interdependent sectors, and with government partners.

Reliability Assessment & Performance Analysis

The Reliability Assessment and Performance Analysis program assesses, measures and investigates historic trends and future projections to improve bulk power system reliability.

- NERC Homepage (www.nerc.com)
 - Survey Results Addressed: Update Compliance Guidance Webpage



The screenshot shows the NERC homepage. The navigation bar includes links for About NERC, Governance, Committees, Program Areas & Departments (highlighted with a red circle), Standards, Initiatives, Filings & Orders, and Newsroom. A red arrow points from the 'Program Areas & Departments' link to a dropdown menu containing the following items: Compliance & Enforcement, Organization Registration and Certification, Standards, Electricity ISAC, Reliability Assessment & Performance Analysis, Reliability Risk Management, and System Operator Certification & Credential Maintenance Program.

The main content area features a large image of power lines and a text block stating: "The North American Electric Reliability Organization Enterprise, which is comprised of NERC and the six Regional Entities, is secure North American bulk power system. Our mission is to assure the effective and efficient reliability and security of the grid."

Below the main content area, there are several sections:

- Headlines & News:**
 - ▶ APPA, E-ISAC Partner on Cybersecurity Summit November 13, 2020
 - ▶ Robb to Participate in New England-Canada Business Council Conference November 09, 2020
 - ▶ Collaboration, Coordination Key to Success in Addressing Risks November 05, 2020
 - ▶ Cancel to Address Senior Canadian Electricity Executives November 02, 2020
 - ▶ ERO Enterprise Further Extends Self-Logging Program Expansion and Deferment of On-Site Activities October 27, 2020
 - ▶ Statement on FERC's October Open Meeting Action October 15, 2020
- Calendar:**
 - Standards
 - Reliability Risk Management
 - Reliability Assessment & Performance Analysis
 - Compliance
 - Board of Trustees
 - System Operator Certification and Continuing Education
 - View All Events
- Standards:**
 - NERC's Standards program ensures the reliability of the bulk power system by developing quality reliability standards in a timely manner that are effective, clear, consistent and technically sound.
- Electricity ISAC:**
 - E-ISAC gathers security information, coordinates incident management, and communicates mitigation strategies with stakeholders within the electricity industry, across interdependent sectors, and with government partners.
- Reliability Assessment & Performance Analysis:**
 - The Reliability Assessment and Performance Analysis program assesses, measures and investigates historic trends and future projections to improve bulk power system reliability.

- NERC Compliance Webpage
 - Survey Results Addressed: Update Compliance Guidance Webpage

The screenshot shows the NERC website's 'Compliance & Enforcement' page. The left sidebar contains a list of links, with 'Compliance Guidance' highlighted by a red circle. The main content area features a breadcrumb trail 'Home > Program Areas & Departments > Compliance & Enforcement', a title 'Compliance & Enforcement', and several informational paragraphs. A right sidebar contains links for 'Program Contacts', 'Calendar', and 'Standards, Compliance, and Enforcement Bulletins'.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Search...
Account Log In/Register | Contact Us

About NERC | Governance | Committees | Program Areas & Departments | Standards | Initiatives | Filings & Orders | Newsroom

Home > Program Areas & Departments > Compliance & Enforcement

Compliance & Enforcement

NERC's compliance efforts are comprised of key activities.

Compliance Monitoring is the process used to assess, investigate, evaluate, and audit in order to measure compliance with NERC Reliability Standards. Standards are developed, adopted, and approved through the Reliability Standards Development program and placed into effect pursuant to FERC orders or to applicable authorities in other North American jurisdictions. This statutory responsibility is set forth in section 215(e) of the Federal Power Act as well as 18 C.F.R. §39.7.

Compliance Enforcement is the process by which NERC issues sanctions and ensures mitigation of confirmed violations of mandatory NERC Reliability Standards. As part of these efforts, NERC can also issue directives to immediately address and deter new or further violations, irrespective of their presence or status (i.e., confirmed or alleged). Sanctioning of confirmed violations is determined pursuant to the NERC Sanction Guidelines and is based heavily upon the Violation Risk Factors and Violation Severity Levels of the standards requirements violated and the violations' duration. Entities found in violation of any standard must submit a mitigation plan for approval by NERC and, once approved, must execute this plan as submitted.

Regional Entity Compliance Monitoring and Enforcement Programs NERC relies on the Regional Entities to enforce the NERC Reliability Standards with bulk power system owners, operators, and users through approved regional delegation agreements. Regional Entities are responsible for monitoring compliance of the registered entities within their regional boundaries, assuring mitigation of all violations of approved Reliability Standards and assessing penalties and sanctions for failure to comply.

Regional hearing processes are available to resolve contested violations or penalties or sanctions. If resolution cannot be achieved at the regional level, NERC maintains an appeals process to hear disputes.

Registered entities or other relevant industry stakeholders can report any perceived inconsistency in the methods, practices, or tools of two or more Regional Entities through the Consistency Reporting Tool located on the [ERO Enterprise Program Alignment Process](#) page.

Who Must Comply?
All bulk power system owners, operators, and users must comply with NERC-approved

Program Contacts

- NERC Certification
- NERC Registration
- NERC Enforcement

Calendar

View Compliance Events

Standards, Compliance, and Enforcement Bulletins

- Standards, Compliance, and Enforcement Bulletin - November 16–22, 2020
November 16, 2020
- Standards, Compliance, and Enforcement Bulletin - November 9–15, 2020
November 09, 2020
- Standards, Compliance, and Enforcement Bulletin - November 2–8, 2020
November 02, 2020
- Standards, Compliance, and Enforcement Bulletin - October 26–November 1, 2020
October 26, 2020
- Standards, Compliance, and Enforcement Bulletin - October 19–25, 2020
October 19, 2020

More Standards, Compliance, and Enforcement Bulletins

- NERC Compliance Guidance Webpage
 - Survey Results Addressed: Update Compliance Guidance Webpage

The screenshot shows the NERC Compliance Guidance Webpage. The page has a blue header with the NERC logo and navigation links. A search bar is in the top right. The main content area is titled 'Compliance Guidance' and includes a sidebar on the left with various links. The main text area contains information about the Compliance Guidance Policy and Implementation Guidance. A table of Implementation Guidance is shown at the bottom.

1 Key Resources

2 Implementation Guidance

3 CMEP Practice Guides

Title	Date	Standards Family
ERO Enterprise-Endorsed Implementation Guidance (31)		
ERO Enterprise-Endorsed Implementation Guidance for Inactive Reliability Standards (1)		
ERO Enterprise-Endorsed Implementation Guidance (2)		
CMEP Practice Guide Phased Implementation Completion Percentages	3/24/2017	
CMEP Practice Guide: Deferral for Implementation Guidance	5/20/2016	

- NERC Compliance Guidance Webpage
 - Key Resources



- NERC Compliance Guidance Webpage
 - Implementation Guidance

2 Implementation Guidance			
Type	Title	Date	Standards Family
<div> <div> <div></div> <div>ERO Enterprise-Endorsed Implementation Guidance (22)</div> </div> <div> <div></div> <div>CIP (12)</div> </div> <div> <div></div> <div>FAC (2)</div> </div> <div> <div></div> <div>PRC (4)</div> </div> <div> <div></div> <div>TOP (3)</div> <div> <div></div> <div>TOP-001-4 and IRO-002-5 Data Exchange Infrastructure and Testing (OC)</div> <div>TOP-010-1(i) R3 and IRO-018-1(i) R2 - RTA Quality of Analysis (OC)</div> <div>TOP-001-3 R13 and IRO-008-2 R4 Real Time Assessments (OC)</div> </div> <div> <div></div> <div>TPL (1)</div> </div> </div> </div>			
<div> <div> <div></div> <div>ERO Enterprise-Endorsed Implementation Guidance for Inactive Reliability Standards (1)</div> </div> </div>			
<div> <div> <div></div> <div>Proposed Implementation Guidance (1)</div> </div> <div> <div></div> <div>PRC (1)</div> </div> </div>			

- NERC Compliance Guidance Webpage
 - CMEP Practice Guides

3 **CMEP Practice Guides**

Type	Title	Date	Standards Family
	CMEP Practice Guide Phased Implementation Completion Percentages	3/24/2017	
	CMEP Practice Guide: Deference for Implementation Guidance	5/20/2016	
	CMEP Practice Guide TOP-001-4 and IRO-002-5 Redundant and Diversely Routed	7/11/2018	TOP
	CMEP Practice Guide Information to be Considered by CMEP Staff Regarding Inverter-Based Resources_V1.1	3/15/2019	
	CMEP Practice Guide Calendar Month Annual	4/19/2019	
	CMEP Practice Guide BES Cyber System Information	4/26/2019	CIP
	CMEP Practice Guide Evaluation of Facility Ratings and System Operating Limits	6/17/2020	FAC
	CMEP Practice Guide TOP-002-4, R6, R7 Determination of Provisions of Operating Plans	7/15/2020	TOP
	CMEP Practice Guide Regarding Inverter-Based Resources	7/15/2020	
	CMEP Practice Guide - CIP-002-5.1a R1 - Generation Segmentation	9/15/2020	CIP
	CMEP Practice Guide - CIP-007-6 R1 Part 1.1 - SVCHost	9/15/2020	CIP



Questions and Answers

CIP-012-1 Communications Between Control Centers

Michael Bilheimer

Senior CIP Analyst





CIP-012-1 Effective Dates





CIP-012 Objective

Purpose: To protect the confidentiality and integrity of Real-time Assessment (RTA) and Real-time monitoring (RTM) data transmitted between Control Centers

NERC Definition: One or more facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability tasks, including their associated data centers, of: One or more facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability tasks, including their associated data centers, of:

- 1) a Reliability Coordinator,
- 2) a Balancing Authority,
- 3) a Transmission Operator for transmission Facilities at two or more locations, or
- 4) a Generator Operator for generation Facilities at two or more location

Applicability: BA, GO, GOP, RC, TOP, TO



CIP-012-1 Requirement 1

The Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between any applicable Control Centers. The Responsible Entity is not required to include oral communications in its plan. The plan shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

- **1.1.** Identification of security protection used to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers;
- **1.2.** Identification of where the Responsible Entity applied security protection for transmitting Real-time Assessment and Real-time monitoring data between Control Centers; and
- **1.3.** If the Control Centers are owned or operated by different Responsible Entities, identification of the responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between those Control Centers.



High Level Required Actions



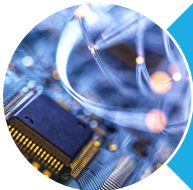
Documented Plan(s)



Identification of Security Protection



Identification of Applied Security Protection



Corporation between Entities Exchanging RTA and RTM
information between Control Centers



Questions

Control Center Definition:

- **NERC Glossary of Terms**

- Facility - Defined
- Data Center – Not Defined
- RTA/RTM – RTA –Defined/ RTM- Not Defined
- Reliability Task –Not Defined.

Defining a Generation Facility as One or Two Facilities

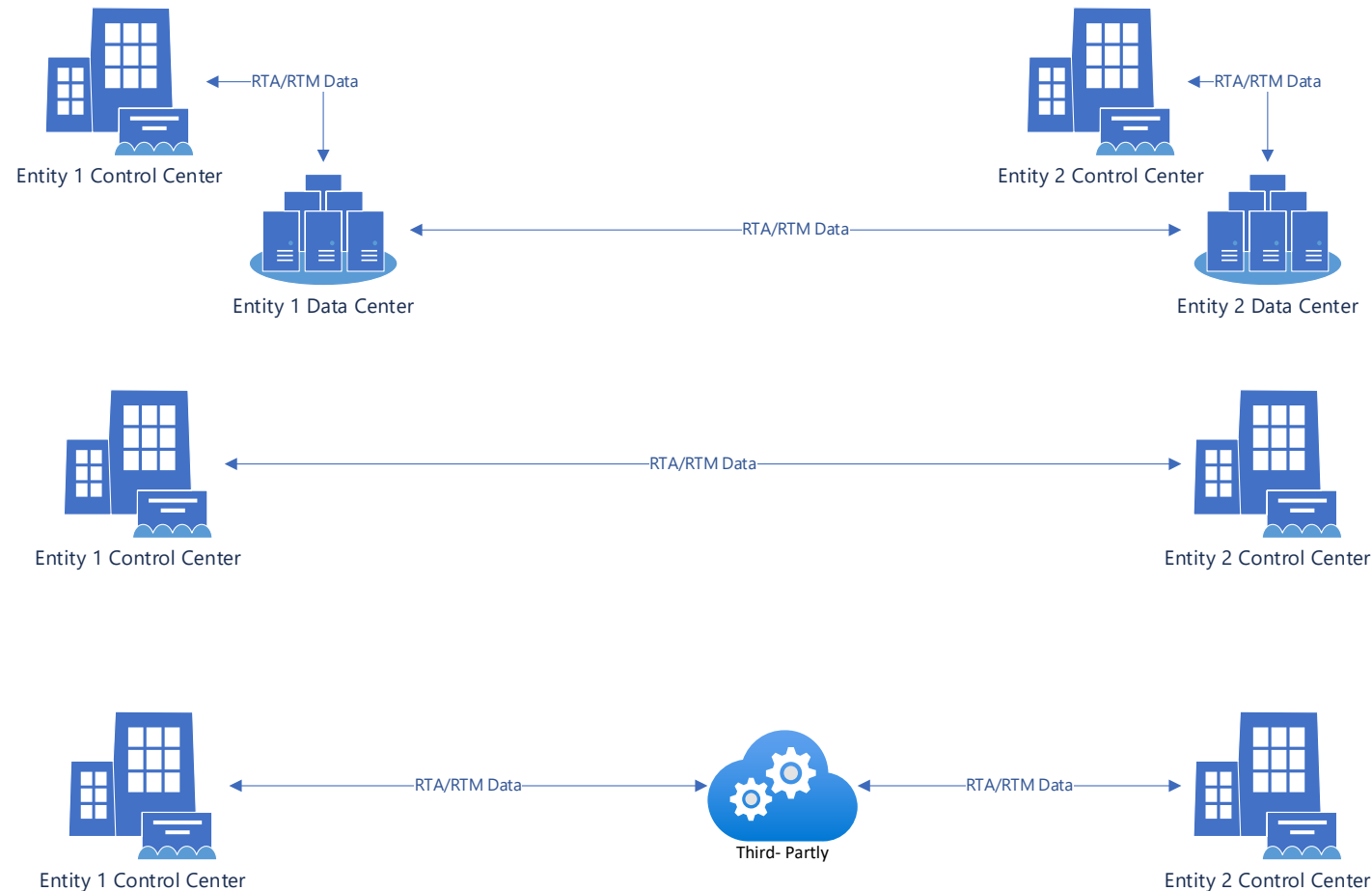
- Interconnection
- Geographic Separation
- Unique Situations

NPCC Specific Diagrams for CIP-012

- NPCC has not developed specific diagrams for CIP-012 beyond ERO endorsed diagrams

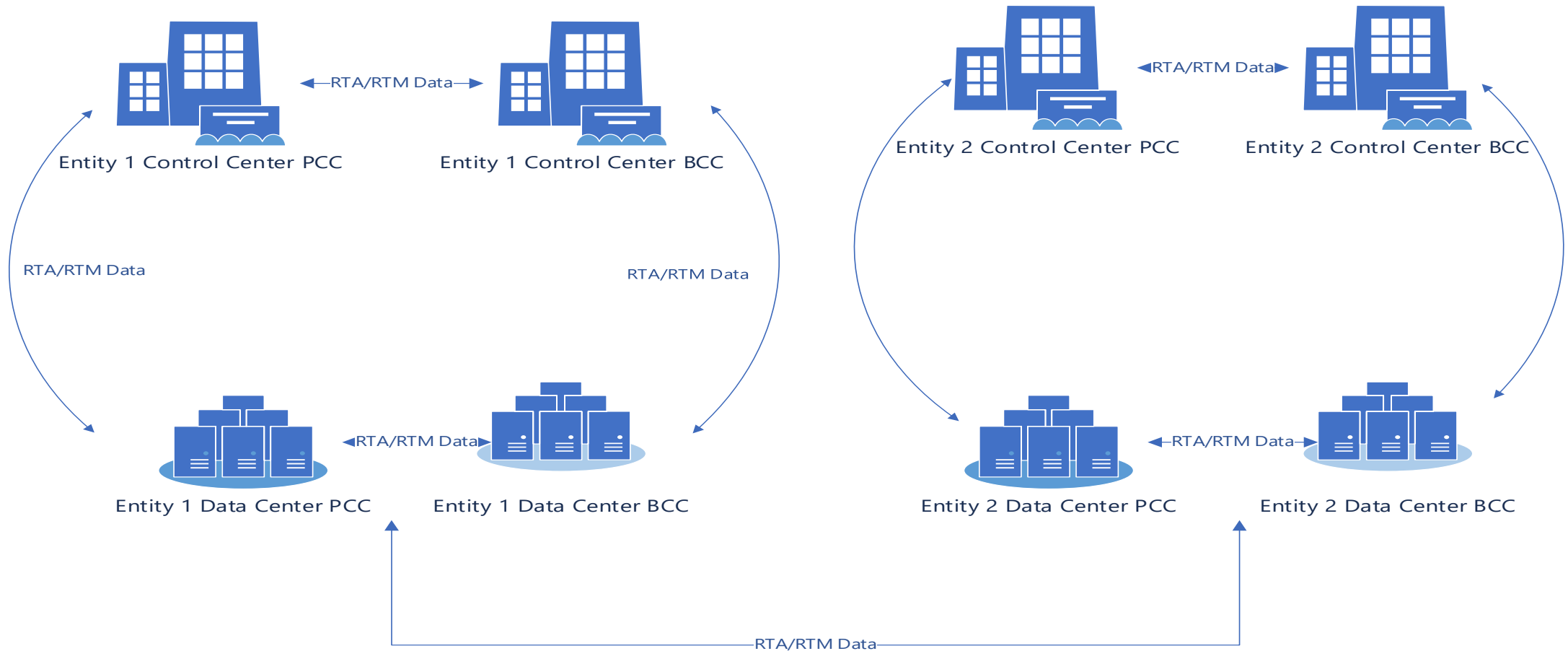


Generic Diagrams Two Entities



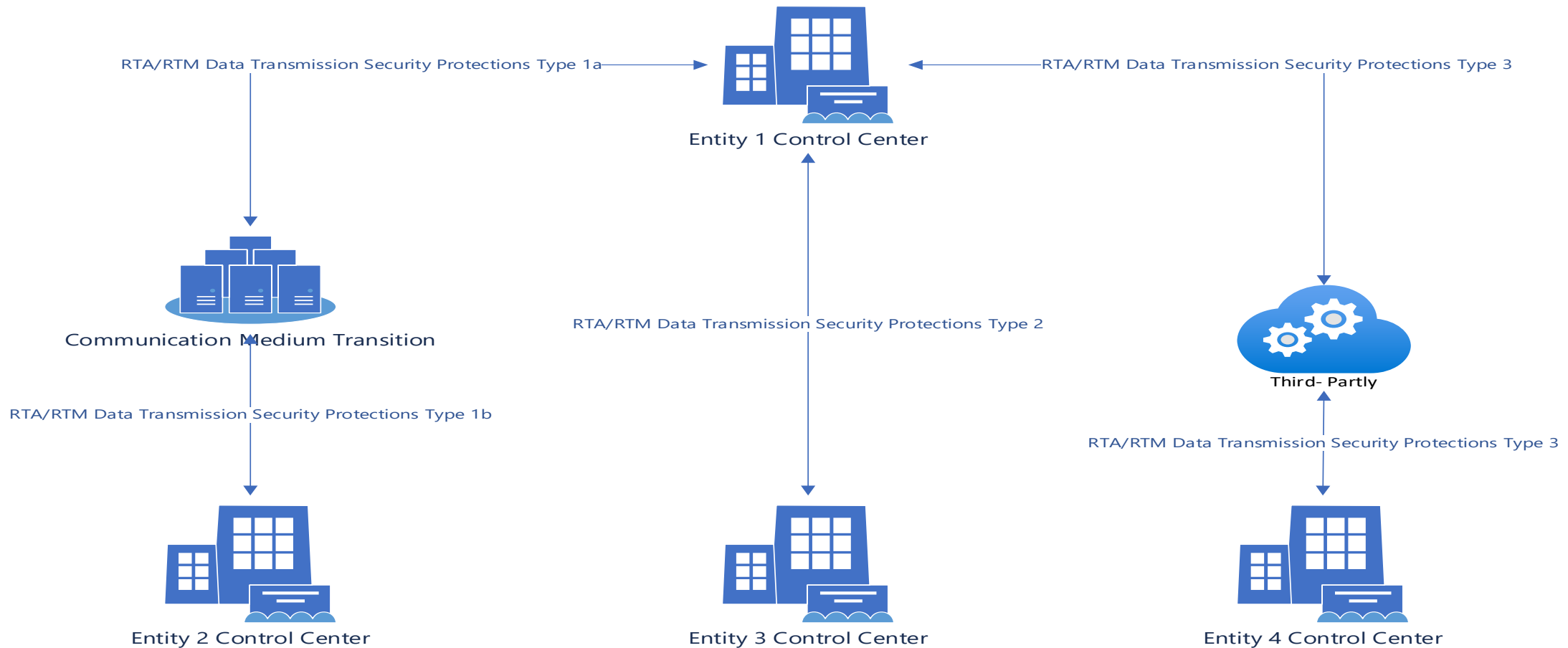


Generic Diagrams 2: Internal and External Transmission





Generic Diagrams 3: Multi - Transmission





Key CIP-012-1 Resources

ERO Endorsed CIP-012-1 Compliance Guidance

NERC CIP-012 Small Group Advisory Session Webinar | **March 8, 2022:** Presentation | Streaming Webinar | **June 2, 2022:** Presentation | Streaming Webinar

NERC CIP-012 FAQ

CIP-012 RSAW

NPCC Whitepaper on NERC Reliability Standard CIP-012(Not ERO Endorsed)

Texas RE 2022 Spring Standards Workshop Presentation | Streaming Webinar

Contact NPCC Compliance: compliance-support@npcc.org



Auditors Compliance Assessment Approach Specifics

R1

- Verify the Responsible Entity has identified any applicable Control Centers.

R1

- Verify the Responsible Entity has identified the transmission of RTA and RTM data between any applicable Control Centers.

R1.1

- Verify the documented plan(s) includes identification of security protection.

R1.2

- Verify the documented plan(s) includes identification of where the Responsible Entity applied security protection.

R1.3

- If RTA or RTM data is transmitted between any applicable Control Centers owned or operated by different Responsible Entities, verify the documented plan(s) includes identification of the responsibilities of each Responsible Entity(ies).

R1

- Verify the entity has implemented, except under CIP Exceptional Circumstances, the documented plan(s) applying security protection to these transmissions.

R1

- Verify the documented and implemented plan(s) achieves the security objective of mitigating the risks posed by unauthorized disclosure and unauthorized modification of RTA and RTM data while being transmitted between any applicable Control Centers.

R1

- Verify entity declaration of CIP Exceptional Circumstances for CIP-012-1



Questions from the Auditors Entity: General

Provide one or more documented plan(s) to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment (RTA) and Real-time monitoring (RTM) data while being transmitted between any applicable Control Centers.

- Single/Multiple/ by Connection.

How did the entity determine communication paths for RTA / RTM?

- What methods were used.

Did the Entity establish any agreements between connected control centers?

- Were any new agreements established for CIP-012 compliance?

How are the list of control centers that the Entity communicates with maintained? How does the entity track Control Centers exchanging RTA / RTM with the entity?

- Static or Actively maintained.

What is the CIP Exceptional Circumstance (CEC) policy and/or process? What is the CIP-012 expectation for CEC handling?



Questions R1

Evidence:

- Provide a description (diagram and/or narrative) of the of the entity communication paths with demarcation between CIP-012 responsibilities between entities including?
- Provide a description (diagram and/or narrative) of the Entity established mitigation measures and where are they applied.

Controls

- How does your entity determine if the security controls have been and are implemented?
- What type of monitoring do you have for the security controls that have been implemented?
- Does your entity preform review of the CIP-012 mitigation measures to determine if they are still effective?



Encryption Evidence



When using encryption provide evidence:

- Config files (all or applicable encryption configuration files)
- Entity demonstrates security controls active For each RTA and RTM transmission segment
 - Inter Entity
 - Entity to Entity
 - Entity ↔ 3RD Party ↔ Entity



3rd Party

Describe third party Company structure.

What is meant by Vendor Diverse Electronic Network?

Describe what “scalable private MPLS network” means to the third-party Network.

How is route diversity determined when connecting to an entity?

How is route diversity determined when connecting to an entity?

What management responsibilities does the third-party communication Carrier has and what are the responsibilities of the Entity?

Is there defined physical security requirements for “third-party Member Location: Physical secure Area.”

Provide a diagram of the of the third-party communication paths with demarcation between responsibilities of the third party and Entity.

Provide assessment or testing of third-party implemented security controls.

What are the third-party supply chain process and protections?



3rd Party Control Questions

What are the responsibilities of the third-party vendor and/or the entity to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data? If encryption is utilized for protecting the data between Control Centers:

- What evidence is supplied that encryption is established?
- What is the notification process if encryption is fails?

If not using encryption, how does the third party notify the entity of Security controls failure?

Provide assessment or testing of third party implemented security controls.

- What reviews are conducted to determine if the third party implemented mitigation controls are effective?

Provide The 3rd party Information Security Policy.

What is the CIP Exceptional Circumstance (CEC) policy and/or process for third party if different from the entity process?

What are the third-party supply chain process and protections? This is a controls question



CIP-012-2

- Project 2020-04 Modifications to CIP-012

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Search...
Account Log-In/Register | Contact Us

About NERC | Career Opportunities | Governance | Committees | Program Areas & Departments | Standards | Initiatives | Reports | Filings & Orders | Newsroom

Home > Program Areas & Departments > Standards > Project 2020-04 Modifications to CIP-012

Project 2020-04 Modifications to CIP-012

Related Files

Status
A formal comment period for **Project 2020-04 Modifications to CIP-012** is open through **8 p.m. Eastern, Wednesday, November 16, 2022** for the following standard and implementation plan:

- CIP-012-2 – Cyber Security – Communications between Control Centers
- Implementation Plan

Additional ballots and non-binding polls of the associated Violation Risk Factors and Violation Severity Levels will be conducted **November 7 – 16, 2022**.

Background
In Order No. 866, FERC stated that “maintaining the availability of communication networks and data should include provisions for incident recovery and continuity of operations in a responsible entity’s compliance plan.” FERC recognized that the redundancy of communication links cannot always be guaranteed, and acknowledged there should be plans for both recovery of compromised communication links and use of backup communication capability. The proposed scope of this project would entail modifications to CIP-012 – Communications between Control Centers.

Standard(s) Affected – [CIP-012](#) - Cyber Security – Communications between Control Centers

Purpose/Industry
The purpose of this project is to address a directive issued by the Federal Energy Regulatory Commission (FERC) in Order No. 866 to develop modifications to the CIP Reliability Standards to require protections regarding the availability of communication links and data communicated between the bulk electric system Control Centers.

Subscribe to this project’s observer distribution list
Select “NERC Email Distribution Lists” from the “Service” drop-down menu and specify “Project 2020-04 Modifications to CIP-012 Observer List” in the Description Box

Draft	Actions	Dates	Results	Consideration of Comments
Draft 3 CIP-012 Clean Redline to Last Posted Redline to Last Approved Implementation Plan Clean Redline to Last Posted Supporting Materials	Additional Ballot and Non-binding Poll Info Vote	11/07/22 – 11/16/22		



Compliance Monitoring Program Updates

Jacqueline Jimenez

Director, Compliance

Emily Stuetzle, CISA

Senior CIP Analyst

Travis Tate

Senior Compliance Engineer





Agenda

2023 Audit Schedule

Hybrid On-site Activity Update

2023 Self-Certification Schedule

Audit and Self-Certification Updates

Updated Audit Milestones Document

NPCC Audit Team

Unplanned CIP Categorization Changes

CIP-014 Update



2023 Audit Schedule

2023 Audit Schedule Posted on NPCC website

- <https://www.npcc.org/program-areas/compliance/monitoring/compliance-audit-schedule>
- 6 On-site Audits
- 12 Off-site Audits

Document Name	Size	Date
2022 Audit Schedule	686.3 KB	11/01/2021
2023 Audit Schedule	192.4 KB	10/24/2022
NPCC Audit Milestones and Deadlines	712.2 KB	11/09/2020



Hybrid On-site Activity Update

On-site activity has resumed



Resumed in Q3
2022

Hybrid audit approach



- Virtual interviews
- On-site inspections
 - Control Center tours
 - Cyber
 - CIP-014
- Small sub-set of audit team

On-site Inspections



- Takes 1 -2 days
- Contain SO interviews
- View EMS screens

Determine entity COVID-19 protocols



Entities must
inform NPCC if they
have any COVID-19
protocols for
visitors



2023 Self-Certification Schedule

2023 Self-Certification Schedule Posted on NPCC website

- <https://www.npcc.org/program-areas/compliance/monitoring/self-cert>
- Self-Certification with evidence
- **Align and the SEL will be used**
- Refer to document for Dates, Standards, and Requirements
- The List of Entities in the schedule are the entities receiving a 2023 Self-Certification
- Notification will be sent 60 days prior to Submittal Period opening
 - This is a change based on the NERC ROP updates
- Entities will have 30 days to respond

The screenshot shows the NPCC website's navigation bar with the 'PROGRAM AREAS' tab selected. Below the navigation bar, the 'Self Cert' section is visible, followed by a 'Documents' section. The 'Documents' section contains a table with two entries. The second entry, '2023 Self-Certification Schedule', is highlighted with a red border.

Document Name	Size	Date
2022 Self-Certification Schedule	223.6 KB	07/05/2022
2023 Self-Certification Schedule	243.4 KB	10/24/2022



Audit and Self-Certification Updates



Based on the NERC Rules of Procedure (ROP) Appendix 4C changes

- Entities will receive at least 270 days notification prior to the commencement of a planned Compliance Audit
- Objections to audit team members must be provided in writing no later than thirty (30) days prior to the start of the Compliance Audit.
- Entities have 30 days to comment on the draft Compliance Audit report
- Entities will receive at least 60 days notification prior to completing a Self-Certification



Updated Audit Milestones Document

Posted on NPCC website

- <https://www.npcc.org/program-areas/compliance/monitoring/compliance-audit-schedule>
- Incorporated ROP changes for Audit Team Member objections
- Clarified type of days
 - i.e., business vs. calendar
- Added “Entity Audit Report comments due” activity



NPCC Audit Team

Jacqueline Jimenez – *Director, Compliance*

O&P Auditors

- Daniel Kidney – *Senior Compliance Engineer*
- Duong Le – *Senior Compliance Engineer*
- George Dong – *Senior Compliance Engineer*
- Kimberly Griffith – *Senior Compliance Engineer*
- Mujahid Mian – *Senior Compliance Engineer*

CIP Auditors

- Anil B. Rauniyar – *Senior CIP Analyst*
- Catherine Nakor-Tetteh – *Compliance Auditor*
- Cecil Elie – *Senior CIP Analyst*
- Emily Stuetzle – *Senior CIP Analyst*
- Michael Bilheimer – *Senior CIP Analyst*

CIP and O&P Auditors

- Patrick Palompo – *Senior Compliance Engineer*
- Travis Tate – *Senior Compliance Engineer*



NORTHEAST POWER COORDINATING COUNCIL, INC.



Unplanned CIP Categorization Changes

Resulting in a Higher Impact Rating

Emily Stuetzle, CISA

Senior CIP Analyst



Planned or Unplanned Changes Resulting in a Higher Categorization

Planned Changes

- Cyber Assets are installed that meet the criteria in CIP-002-5, Attachment 1
- Must be in compliance with the Version 5 CIP Cyber Security Standards upon commissioning



Planned or Unplanned Changes Resulting in a Higher Categorization

Unplanned Changes

- Example: Notification of the change from your ISO
- Must be in compliance with the CIP Cyber Security Standards according to table in the implementation plan



Scenario of Unplanned Changes After the Effective Date	Compliance Implementation
New high impact BES Cyber System	12 months
New medium impact BES Cyber System	12 months
Newly categorized high impact BES Cyber System from medium impact BES Cyber System	12 months for requirements not applicable to Medium-Impact BES Cyber Systems
Newly categorized medium impact BES Cyber System	12 months
Responsible entity identifies first medium impact or high impact BES Cyber System (i.e., the responsible entity previously had no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes)	24 months

[NERC Implementation Plan for Version 5 CIP Cyber Security](#)

(starting at the bottom of page 3)



Unplanned Changes Resulting in Low Impact Categorization

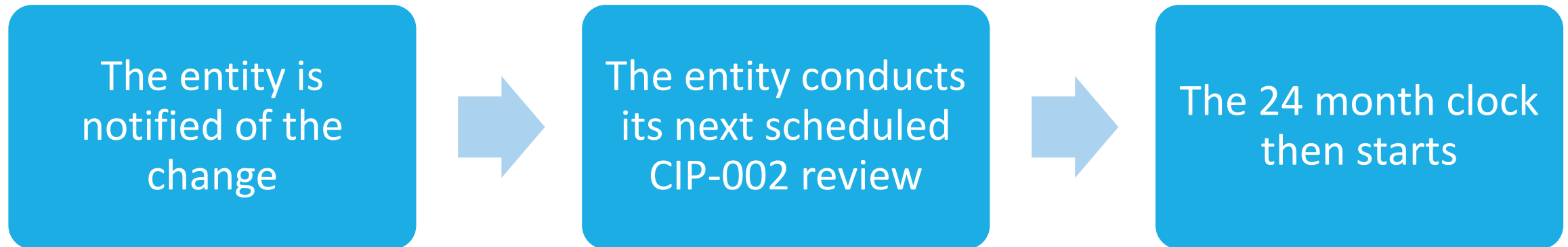
For unplanned changes resulting in a low impact categorization where previously the asset containing BES Cyber Systems had no categorization, the Responsible Entity shall comply with all Requirements applicable to low impact BES Cyber Systems within 12 calendar months following the identification and categorization of the affected BES Cyber System.

[NERC CIP Implementation Plan](#)

(bottom of page 10)



First medium impact or high impact BES Cyber System identified





Periodic Review Examples

Begin after the 24-month clock ends

Standard	Req	Language
CIP-004-6	R4.3	For electronic access, verify at least once every 15 calendar months that...
CIP-008-6	R2.1	Test each Cyber Security Incident response plan(s) at least once every 15 calendar months...
CIP-010-3	R3.1	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.



NORTHEAST POWER COORDINATING COUNCIL, INC.



CIP-014 Update

Travis Tate

Senior Compliance Engineer



Objectives

The History of CIP-014

CMEP Practice Guide highlights

NPCC Audit Guidance



The History of CIP-014

In 2013, the Metcalf substation located in Central California suffered catastrophic damage from multiple gunshots.

- Over 100 gunshots within 19min.
- Thousands of gallons of oil was spilled.
- \$15 million worth of damage.
- To date no attackers were caught.

In 2013, FERC ordered NERC to develop a physical security standard within 90 days, to enhance physical security measures for critical BES facilities.



CMEP Practice Guide CIP-014 R1 Highlights

Practice Guide

Posted September
19, 2022

[CMEP Practice Guide
CIP-014-2 \(nerc.com\)](https://www.nerc.com/cmepractices/CIP-014-2)

Applicability List

How Entities develop
and maintain an
applicability list as
defined
by Applicability
Section 4.1.1.

Models

How Entities select
and prepare models
to perform their risk
assessment.

Inclusion of facilities
planned to be in
service within 24
months.

Technical Analyses

Ensure the risk
assessments
performed
adequately studies
the loss of
stations that could
result in

- Instability
- Uncontrolled separation
- Cascading



NPCC Audit Guidance

Requirement 1

- Transmission Risk Assessment
 - How do you identify substation(s).
 - What model year are utilized for risk assessments
 - Performed at least **once every 30 calendar** months if stations were previously identified.
 - Performed at least **once every 60 calendar** months if no stations were previously identified.

Requirement 2

- The Third-Party review
 - Should be independent.
 - The third-party reviewer should not dictate how your study is performed.
 - The third-party reviewer can provide suggestions for entities to incorporate in their methodology/ procedure.
 - Performed **within 90 Calendar** days of R1.
 - Can be performed concurrently with R1.



NPCC Audit Guidance (continued)

Requirement 4

- The Vulnerability assessment should consider prior security events.
 - Vandalism and sabotage.
 - Threat warnings from law enforcement, EISAC, other US and Canadian governmental agencies.
- Make sure your prior considerations are up to date or within reason.
 - **Within 120 Days** after completion of R2. (in conjunction with R5)

Requirement 5

- Based off threats and vulnerabilities discovered in R4
- Develop or review a physical security plan designed to deter, detect, assess, communicate, and respond to potential threats.
- A timeline for executing the physical security enhancements and modifications specified in the physical security plan.
 - **Should be performed within 120 calendar days of completion of R2 (Performed in conjunction with R4)**



NPCC Audit Guidance (continued)

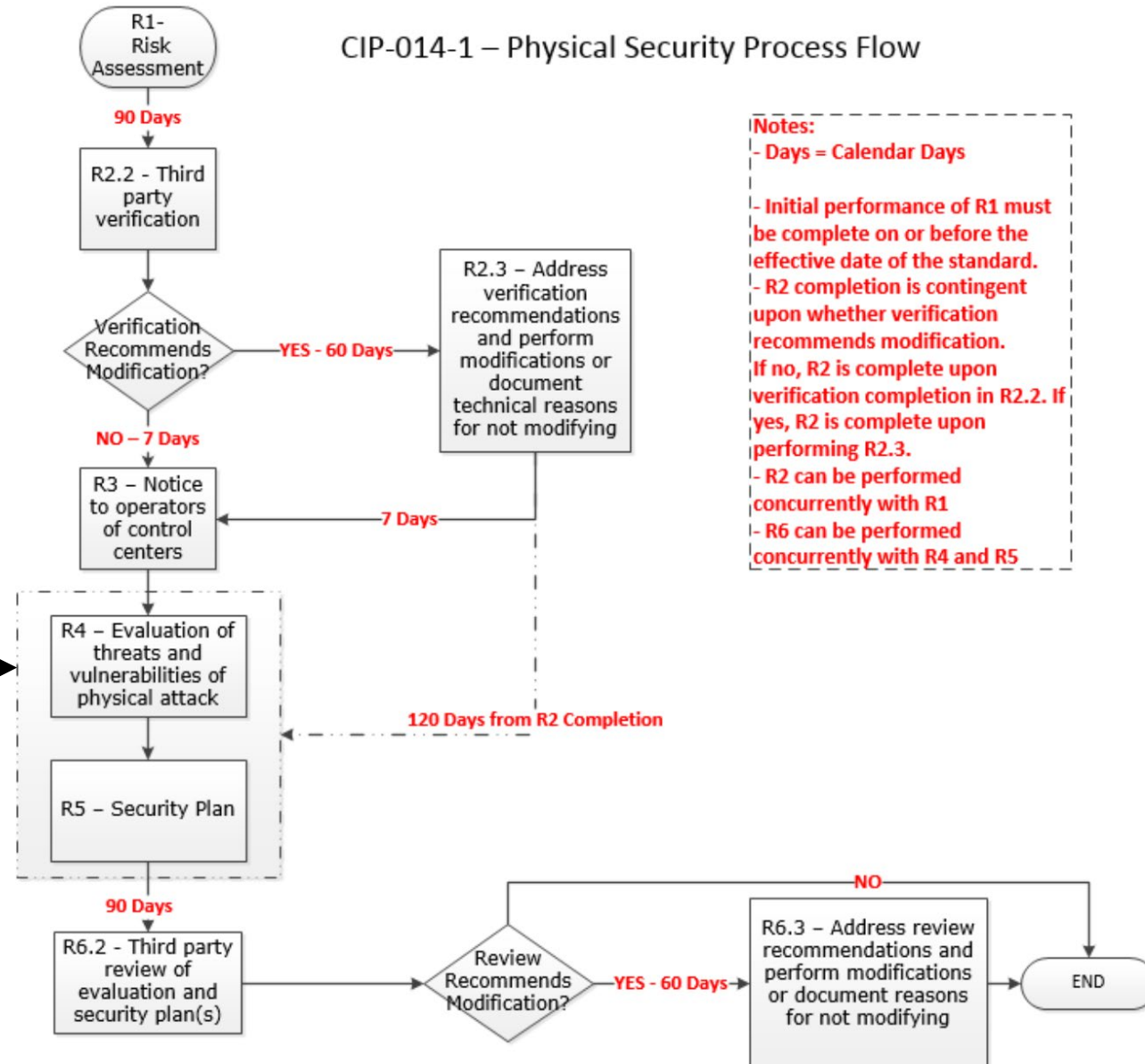
Requirement 6

- Once R4 and R5 are complete the entity must have a qualified unaffiliated third-party review R4 (the vulnerability assessment) and R5 (the physical security plan).
 - **Within 90 days** of completion of R4 and R5.
 - Can be performed concurrently with R4 and R5.
 - R6.3 must be completed **within 60 days** of the R6.2 review recommendations.



CIP-014-1 – Physical Security Process Flow

Standard verbiage for R4 does not specifically state time for completion.





Site Inspections



For Entities with CIP-014 applicable sites:

- The audit team will perform site inspections.



The inspection will be developed based on the Entity's:

- Most recent vulnerability assessment
- Most recent physical security plan



NORTH

COORDINATING COUNCIL, INC.



Questions

Jacqueline Jimenez

jjimenez@npcc.org

Emily Stuetzle

estuetzle@npcc.org

Travis Tate

ttate@npcc.org

PUBLIC

NPCC Cold Weather and Winterization Outreach

Matt Forrest

Senior O&P Entity Risk Analyst

November 9, 2022





- Thanks to all those who participated by responding to the NERC Cold Weather Practice Guide questions for GO/GOP.
- Special thanks to Canal Generating, Dighton Power, Milford Power, Tanner Street Generating, Newington and Schiller Stations, and Lockport Energy for in person and virtual plant tours.



BACKGROUND

Cold Weather continues to be a risk to the BPS despite previous Cold Weather events.

- Investigations
- Reports
- Lessons Learned
- Recommendations
- New / Revised Reliability Standards

The NERC Cold Weather Preparedness CMEP Practice Guide provides a set of questions to allow entities to establish a minimum baseline for cold weather preparedness.

The updated standards provide a set of minimum considerations.

The goal of the outreach is to gather good practices and lessons learned beyond those listed in the standards relative to the GO/GOP function.



STANDARDS

NERC Standards that are becoming enforceable
on APRIL 1ST, 2023

- **IRO - 010 – 4**
- **TOP - 003 - 5**
- **EOP - 011 – 2**



EOP - 011 – 2

R7: Each GO shall implement and maintain one or more weather preparedness plans(s) for its generating units. The weather preparedness shall include, at a minimum:

- 7.1. Generating unit(s) freeze protection measures based on geographical location and plant configuration;
- 7.2. Annual inspection and maintenance of generating unit(s) freeze protection measures
- 7.3. Generating unit(s) cold weather data, to include: (Common language in all three standards.)
 - 7.3.1. Generating unit(s) operating limitations in cold weather to include:
 - 7.3.1.1. capability and availability;
 - 7.3.1.2. fuel supply and inventory concerns;
 - 7.3.1.3. fuel switching capabilities; and
 - 7.3.1.4. environmental constraints.
 - 7.3.2. Generating unit(s) **minimum:**
 - 7.3.2.1. design temperature; or
 - 7.3.2.2. historical operating temperature; **or**
 - 7.3.1.3. current cold weather performance temperature determined by an engineering analysis.



EOP-011-2

- **R8:** Each Generator Owner in conjunction with its Generator Operator shall identify the entity responsible for providing the generating unit-specific training, and that identified entity shall provide the training to its maintenance or operations personnel responsible for implementing cold weather preparedness plan(s) developed pursuant to Requirement R7



Additional Considerations

- Know the basis for generator operating limitations day to day
- Take advantage of affiliates and industry forums.
 - North American Generator Forum
 - North American Transmission Forum
- Annual cold weather plan, maintenance program, operator awareness, and corrective action program.



ESTABLISH PROTECTIVE MEASURES

- Protective measures and efforts should be prioritized based on equipment that has the potential to:
 - Cause unit trip or partial outages.
 - Impact unit start-up or plant monitoring and automation
 - Cause equipment or plant damage
 - Adversely impact the environment.
 - Cause fuel disruption
 - Reduce plant safety



WINTER PREPARATION GOOD PRACTICES

- **Split up winter preparation and planning rather than trying to accomplish it just prior to winter.**
 - **Review prior winter**
 - Effectiveness of cold weather strategy
 - Trouble areas
 - Complete corrective actions and document
 - **Prioritize work orders**
 - Consider a cold weather code
 - Ensure work is scheduled to complete prior to a specific date.
 - **Keep a winterization items list year-round.**
 - **Ensure personnel are trained.**



WINTER PREPARATION GOOD PRACTICES

- Developing a plan - Prioritize your review and preparation.
- Building doors, Building Louvers, Building Heat, GT intake, and boiler stack area
- External Piping, insulation, traps, and heat trace.
- Vital instrumentation
- Fuel Supply
- Plant cooling basins, tank heat
- Main plant condensate, feed, and boiler system, aux boiler
- Emergency Generator and fuel supply, key loads.
- Station service power
- Other systems – instrument air, fire protection, water treatment
- Lessons learned from prior winter events. Corrective Action Plans, Mitigation results, Extent of condition.



WINTER PREPARATION GOOD PRACTICES

- Building doors and louvers and installed heat are the first line of defense.





PROTECTIVE MEASURES

- Pre-stage temporary heaters in areas known to be susceptible to low temperatures.





USE EXISTING PLANT EQUIPMENT OR SYSTEMS

- Two different methods using similar systems at different plants.



- Offline boiler recirc pump



HP economizer drain



USE EXISTING PLANT EQUIPMENT OR SYSTEMS

- Utilize a low load single burner as a keep warm method.
- Look at system prints to see if a condensate pump can be used as a full flow option to circulate all condensate and steam to help keep systems warm.

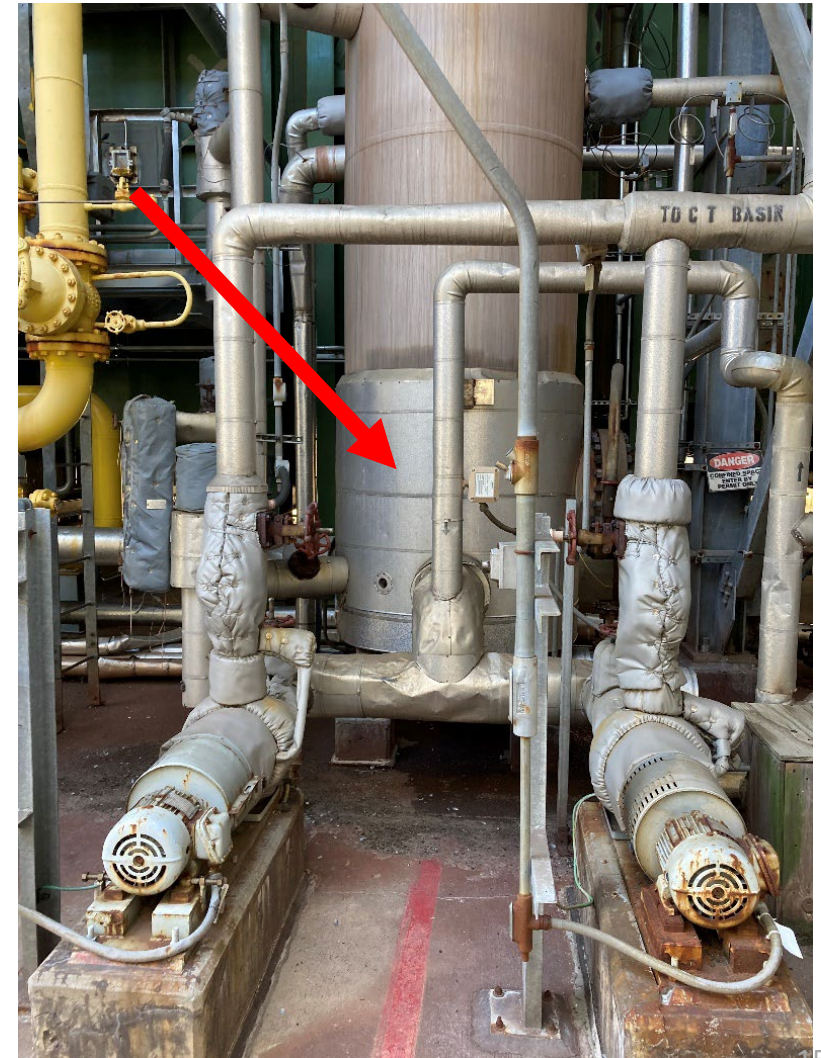




INCREASED MONITORING AND OPERATOR ACTION

The downcomer pictured is periodically drained until warm water flows from the drain.

This is an example of utilizing increased monitoring or additional operator rounds to combat potential freeze issues.





EXTERNAL EQUIPMENT PROTECTION

- Verify the operability heaters, heat trace, and traps.
- Ensure exterior piping insulation is inspected as part of the preparation process and insulation contractors are available to repair prior to winter months. Many plants perform this in the September timeframe.





MULTI-PURPOSE EQUIPMENT



- This electric aux boiler is used for startup to provide steam seals to the turbine.
- Plant operators have been able to repurpose their aux steam to perform plant keep warm functions when off-line.



VITAL EQUIPMENT AND INSTRUMENTS

- Instrument racks can be covered and heated with as little as a small heat lamp or heat strips.
- The front panel can be clear plastic to allow operators easy viewing of system parameters that require local readings.





OPERATOR ROUNDS

- Consider additional checks during winter months.
 - Know and check all single failure equipment and understand plant trip criteria.
 - Get system engineers or maintenance to help operators to look for possible vulnerable areas
 - Monitor Area Temperatures and temporary winter protection.
 - Verifying building penetrations close and seal properly.
 - Look out for damaged or missing insulation.
 - Utilize an IR gun and understand key locations and systems to monitor.
 - Verifying heat trace functionality, steam trap functionality.
 - Maintain a list of deficiencies that require additional contingencies.
 - Eg: failed steam trap or air receiver required frequent blow down

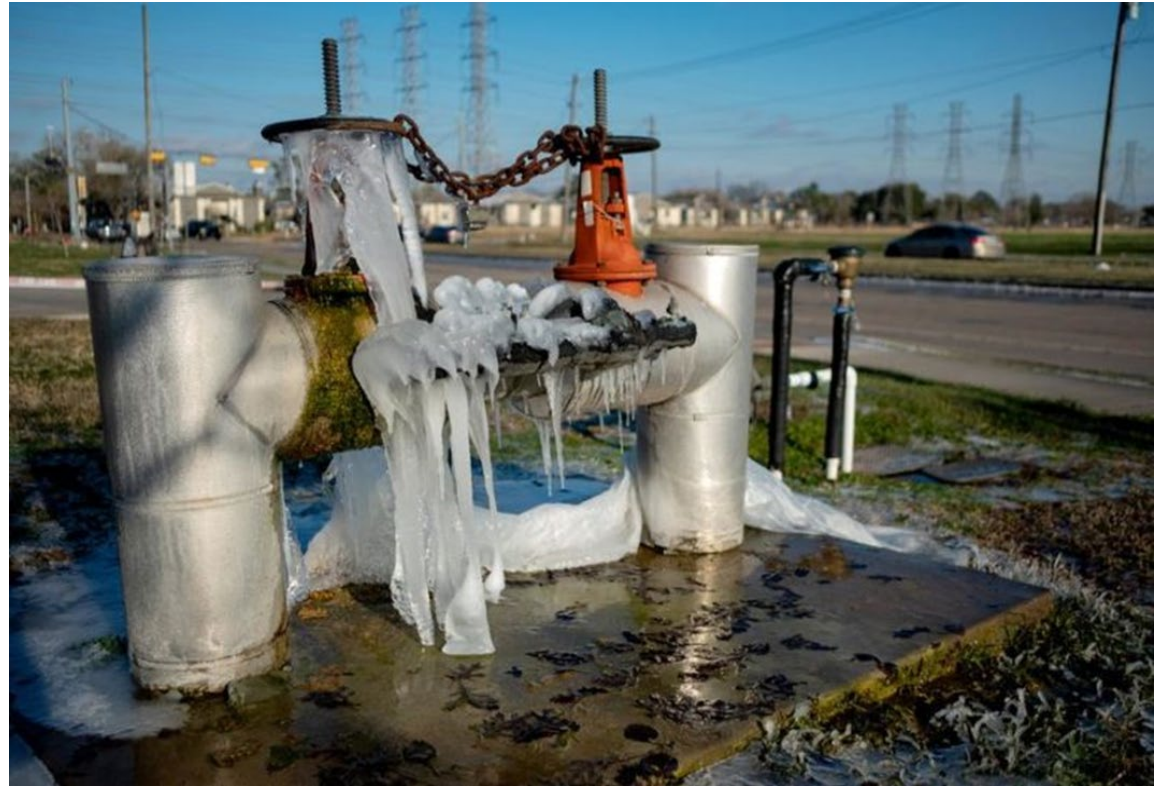


OPERATOR ROUNDS

Ensure that pathways to key equipment are kept clear during snow events.



Minor packing leaks or insulation damage can lead to catastrophic results.





WINTER PREPARATION MAINTENANCE PRACTICES

- Create a seasonal inspection and maintenance program.
 - Establishes equipment work prioritization, processes, and due dates.
- Consider creating a winter work order prioritization code to track all winter items and create completion percentage reports or walkdown lists.
- Establish an early deadline for completion of winter deficiency items. Don't wait until the last minute.
- Prioritize work on systems and equipment needed to cope with winter conditions.
 - Heat trace, insulation, installation of temporary heaters and other cold weather protection measures



SNOW AND ICE CONSIDERATIONS



- Snow and ice can cause a multitude of problems in the power block and substation.
- Wet snow and ice has caused short circuits on insulators causing loss of one or more offsite power sources.
- Falling ice can damage vital equipment and be a personnel safety issue.



OTHER ITEMS TO CONSIDER

- Many plants have done a good job capturing trip critical and main plant systems in their cold weather protection but have failed to look at support or non power generating items.
- Fire protection for example is often located in stair wells, the building perimeter or remote areas of a building that may not be warm enough.
- Get plant personnel buy in.





RECAP OF NERC RECOMMENDATIONS GO/GOP

- There are nine recommendations that came out of Project 2021-07 Extreme Cold Weather Grid Operations, Preparedness, and Coordination. Below are the GO/GOP related items
- Generator Owners are to identify and protect cold-weather-critical components and systems for each generating unit.
- Generator Owners are to design new or retrofit existing generating units to operate to a specified ambient temperature and weather conditions.
- Generator Owners and Generator Operators are to conduct annual unit-specific cold weather preparedness plan training.
- Generator Owners that experience outages, failures to start, or derates due to freezing are to review the generating unit's outage, failure to start, or derate and develop and implement a corrective action plan for the identified equipment and evaluate whether the plan applies to similar equipment for its other generating units.
- Generator Owners are to account for the effects of precipitation and accelerated cooling effect of wind when providing temperature data.



APPENDIX



Additional Considerations

- Basis for generator operating limitation
 - When was the last time you assessed your unit's temperature design parameters?
 - What are historical low temperatures and duration?
 - Is your unit capable of fuel switching?
 - Do you have a process in place to obtain an emissions waiver in the event one is needed to operate?
- Take advantage of affiliates and industry forums.
 - Does your organization conduct fleet-wide annual winter preparation meetings, training exercises, or both to share best practices and lessons learned?
 - Does your organization participate in industry associations to share and gain insights on cold weather preparedness?
- Annual maintenance program and operator awareness.
 - How do you ensure winterization supplies and equipment are in place before the winter season?
 - How do you track operating experience, preventive and corrective winter maintenance, installation of protective measures?
 - Are operator rounds modified?
 - Are operators aware of critical equipment and operating limits?
 - Maintain a freeze protection list.



WINTER PREPARATION GOOD PRACTICES

- **Split up winter preparation and planning rather than trying to accomplish it just prior to winter.**
- Utilize March to May to perform the following:
 - Review the effectiveness of past winter protection and awareness measures.
 - Perform a walkdown to look for recent winter effects and review known deficient areas from prior years.
 - Secure items and systems only needed for the winter. (Track storage locations)
 - Document and schedule any maintenance or refurbishment needed to ensure the equipment is fully functional prior to storage.
 - Prioritize work orders to ensure repairs are completed prior to next winter.
 - Ensure all items are scheduled to be completed prior to an October/November deadline.



WINTER PREPARATION GOOD PRACTICES

- Maintain a winter readiness list. Operators should document deficiencies and ensure they are added to the list and work management schedule.
- Verify contractors for snow removal, insulation repairs etc are set for the following winter.
- September through November:
 - Verify that all winter readiness work orders are completed and closed.
 - Perform final walkdown of vulnerable systems.
 - Generate the PMs for installation of protective measures and start up of systems needed for winter operations. Test and verify functionality.
 - Ensure that PPE and cold weather gear is available for operators and maintenance personnel.
 - Perform “Just in Time” Cold Weather Refresher training.



WINTER PREPARATION GOOD PRACTICES

- Panels and other door or louver covers
- Evaporator Systems that enclose this GT inlets have High Density poly panels that are installed to stop air flow into the Gas Turbine Inlet Filter area. Garage doors are Opened if there is a need to run the unit and closed after Shutdown to complete the inlet isolation.





PROTECTIVE MEASURES

Heaters such as the one pictured can be used to blow air into the back end of a boiler. This is an area that is susceptible to possible freezing even if the stack is equipped with dampers.

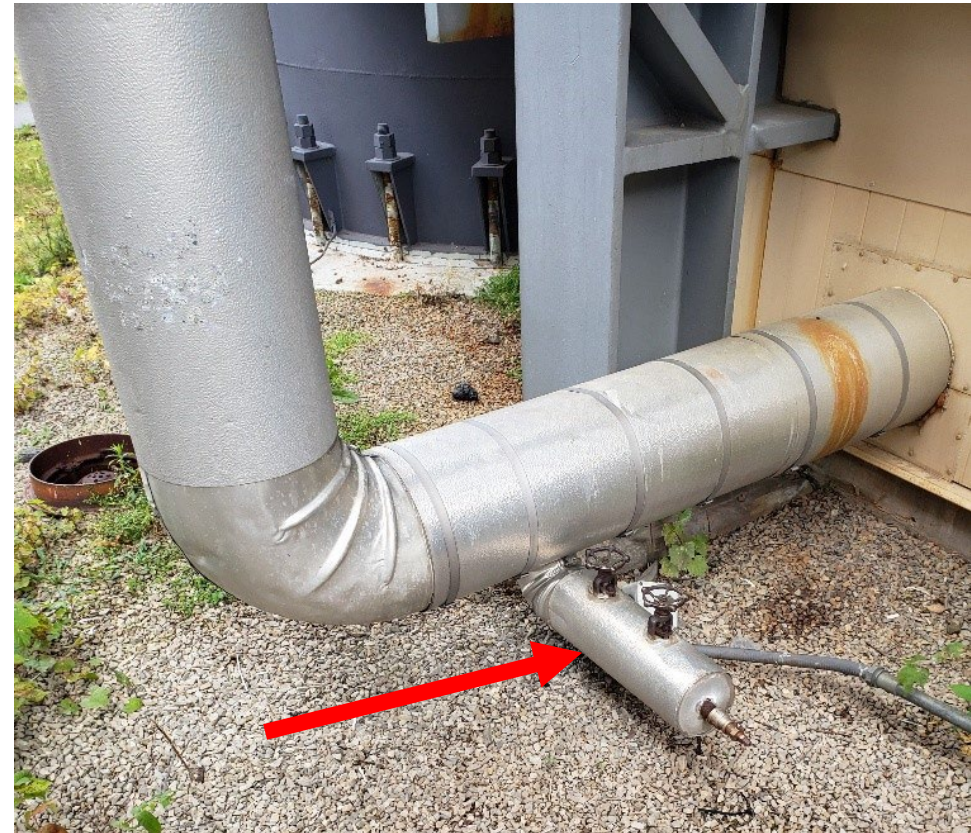
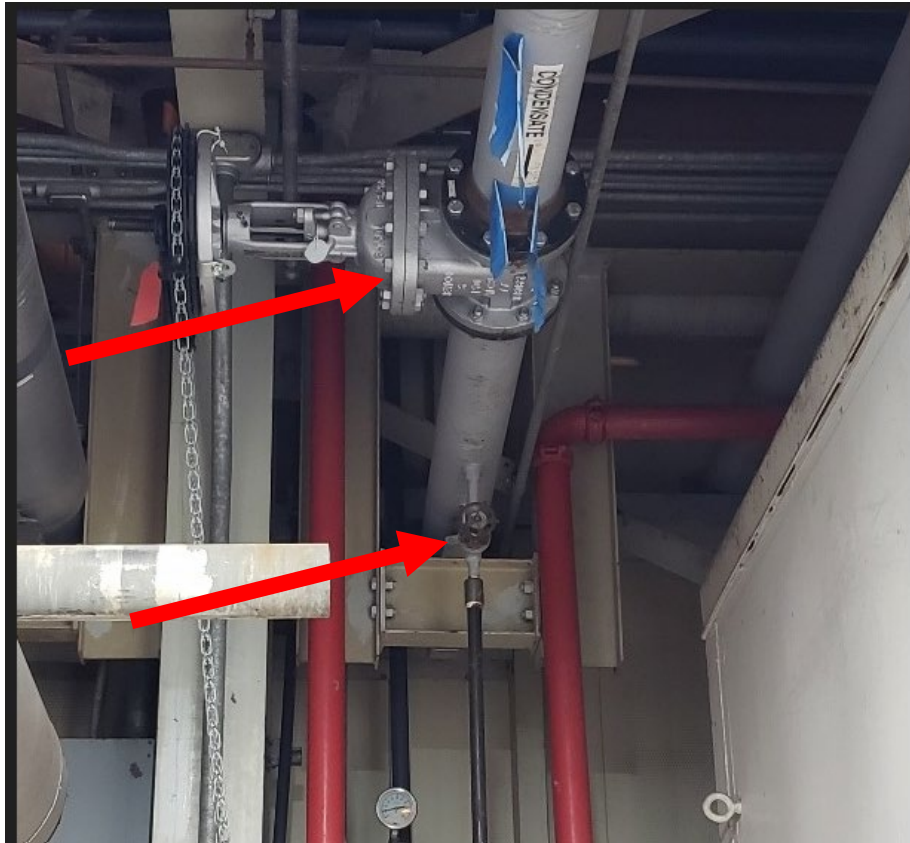
This one is used in conjunction with a small recirc pump to ensure warm water is circulated through the boiler tube and drums.





USE EXISTING PLANT EQUIPMENT OR SYSTEMS

- Utilize existing isolation valves and drains to protect external piping.





MINOR MODIFICATIONS TO EXISTING PLANT SYSTEMS

- Consider plant systems and take advantage of current piping and flow path options.
- Not all modifications need to break the bank or require extensive mods.





EXTERNAL EQUIPMENT PROTECTION

- Keep insulation in mind year-round and track deficiencies. Know where heat trace is located. If insulation is damaged, HT could also be affected.





EXTERNAL EQUIPMENT PROTECTION





EXTERNAL EQUIPMENT PROTECTION





OPERATOR ROUNDS

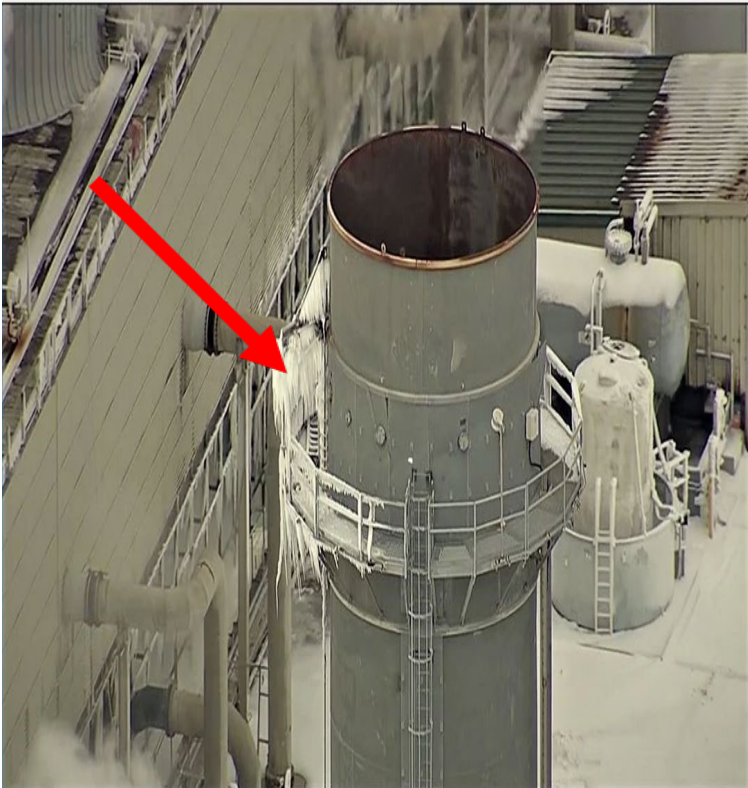
A valve packing leak, damaged insulation or loss of heat trace can escalate quickly to cause equipment damage or plant trip.





SNOW AND ICE CONSIDERATIONS

- Falling ice can cause equipment damage or personnel injury.





OTHER ITEMS TO CONSIDER

- Get plant staff buy in and ideas for cold weather and snow protection ideas.





OT Cyber Threats and The Electric Sector

NPCC Compliance and Reliability Conference

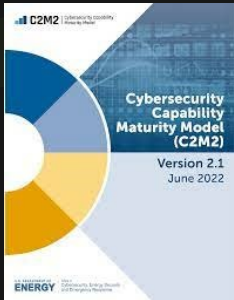
Justin Pascale

Principle Industrial Consultant

jpascale@dragos.com
[in linkedin.com/in/justin-pascale/](https://www.linkedin.com/in/justin-pascale/)

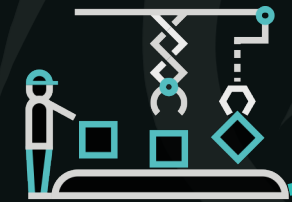


Honeywell



INDUSTRY TRENDS

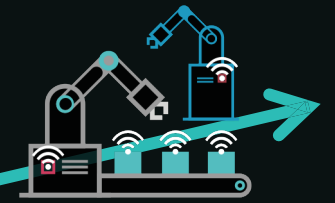
Growing investment in digital transformation and hyperconnectivity



STAND-ALONE



LOOSELY
CONNECTED



HIGHLY
CONNECTED

Greater exposure to
malicious cyberthreats



**"Threat groups are rising 3X
faster than they're declining..."**

Source: Dragos 2021 YIR

Threat Groups

Threat Groups

Who are we talking about?

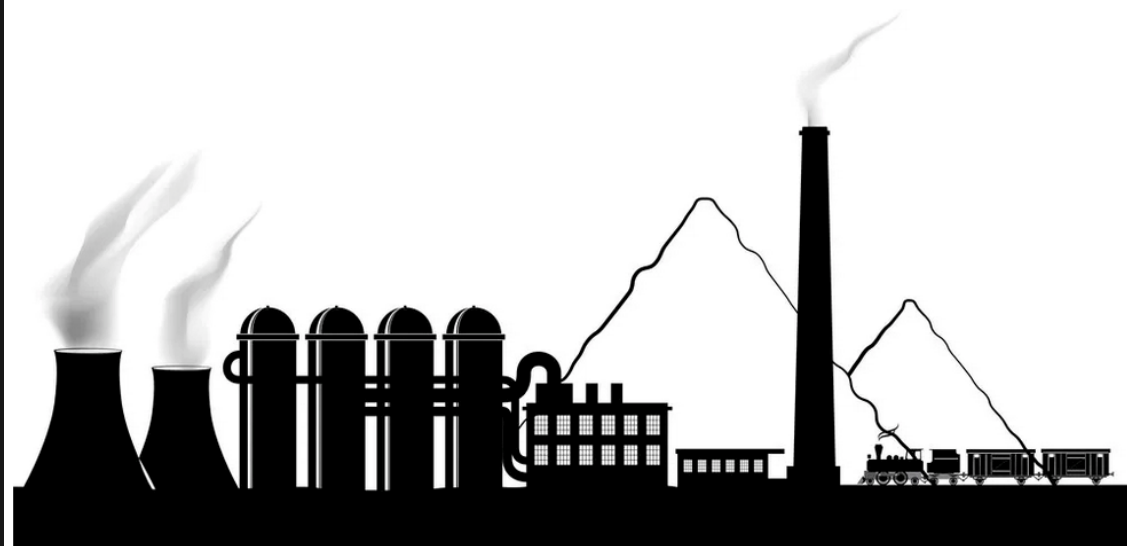
- ▶ ALLANITE
- ▶ CHRYSENE
- ▶ DYMALLOY
- ▶ ELECTRUM
- ▶ KAMACITE
- ▶ MAGNALIUM
- ▶ PARISITE
- ▶ STIBNITE
- ▶ TALONITE
- ▶ WASSONITE
- ▶ XENOTIME



Threat Groups

Generation

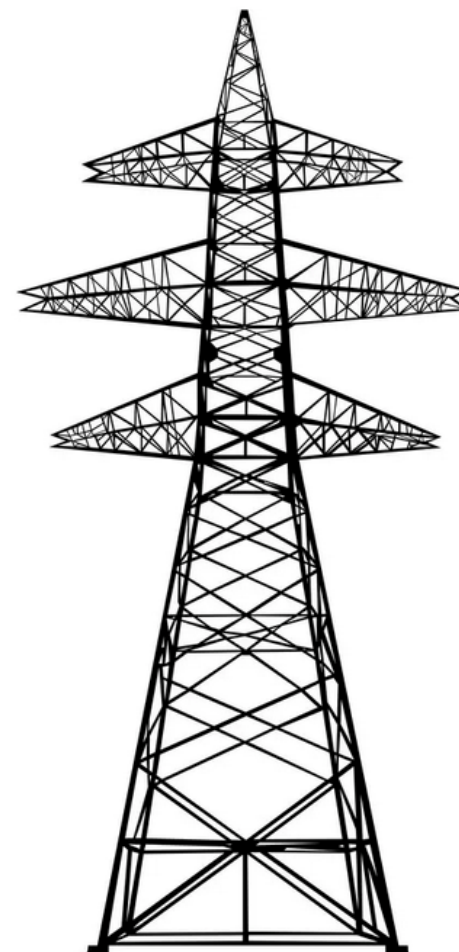
- At least five AGs have demonstrated intent or capabilities to impact generation
- OT-targeting adversaries have not successfully disrupted electric power generation.
- Increased reconnaissance efforts demonstrate desire to conduct espionage and/or cyber-physical attacks



Threat Groups

Transmission

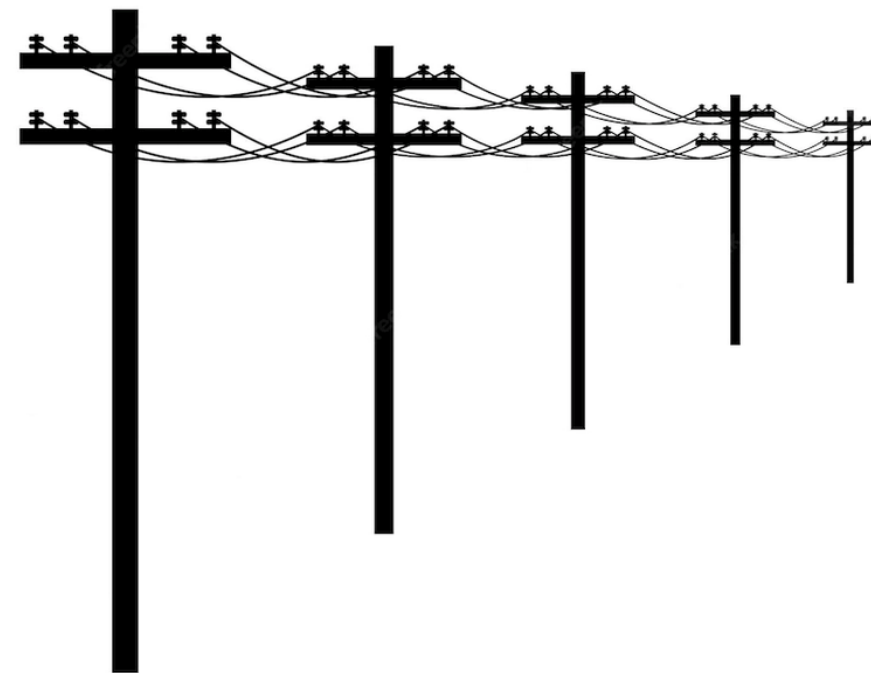
- At least two AGs are a threat to transmission operations
- CRASHOVERRIDE targeted breaker operations controlled by ABB devices adhering to the IEC 61850 standard
- PIPEDREAM shows a trend towards threat groups developing more modular malware



Threat Groups

Distribution

- First widespread outage caused by a cyberattack (Ukraine 2015)
- Contrary to ELECTRUM, the adversary did not use ICS-specific malware
- The behaviors and tools use exhibited could be deployed in distribution operations globally depending on the adversary sponsor's focus



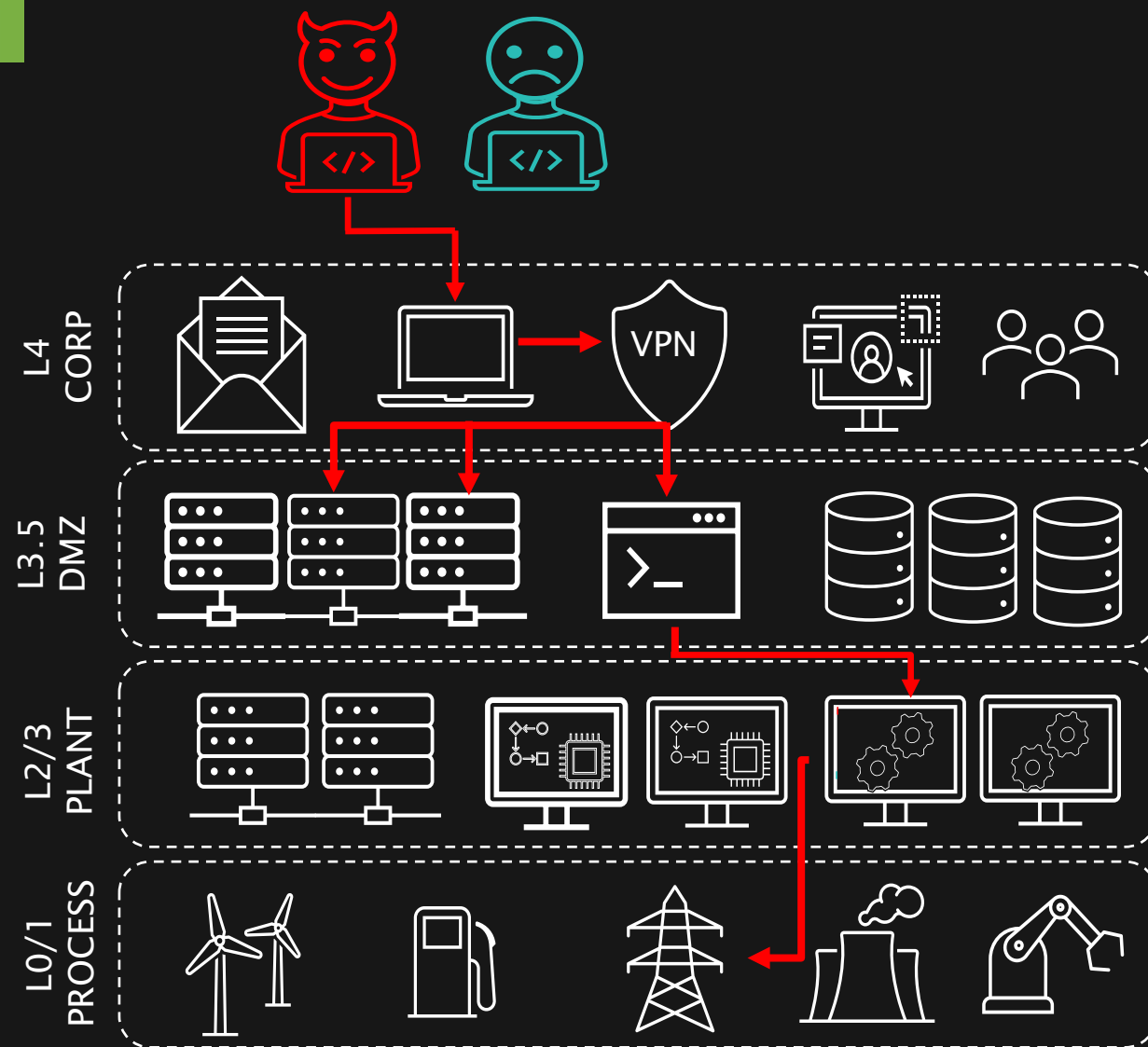
The background features a dark, industrial scene with a complex metal structure, possibly a crane or part of a large machine. Overlaid on this are faint, light-colored technical drawings and circuit-like patterns, including lines, dots, and circular motifs, suggesting a high-tech or engineering theme.

Supply Chain and Remote Access

Third Parties

When three's a crowd

- Third Parties often have remote access to critical parts of customer networks
 - XENOTIME and ELECTRUM have increased reconnaissance efforts targeting third parties
- Compromising a trusted third party magnifies the potential risks to infrastructure
 - HAVEX targeted over 2000 industrial sites—with a large emphasis on electric power asset owners

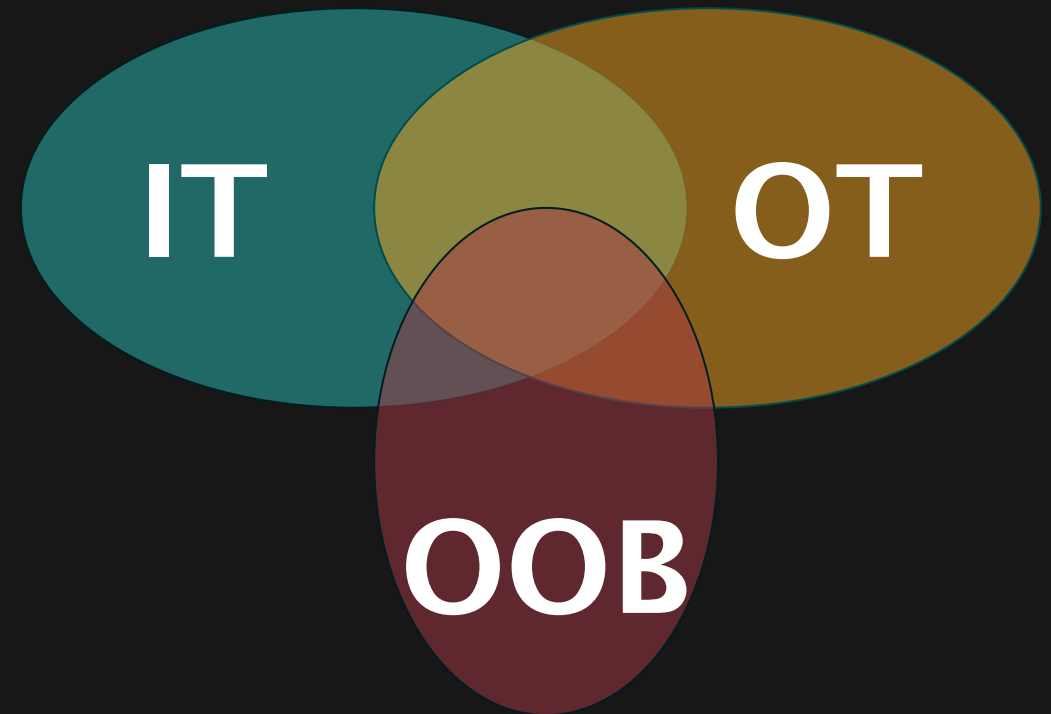


Ransomware

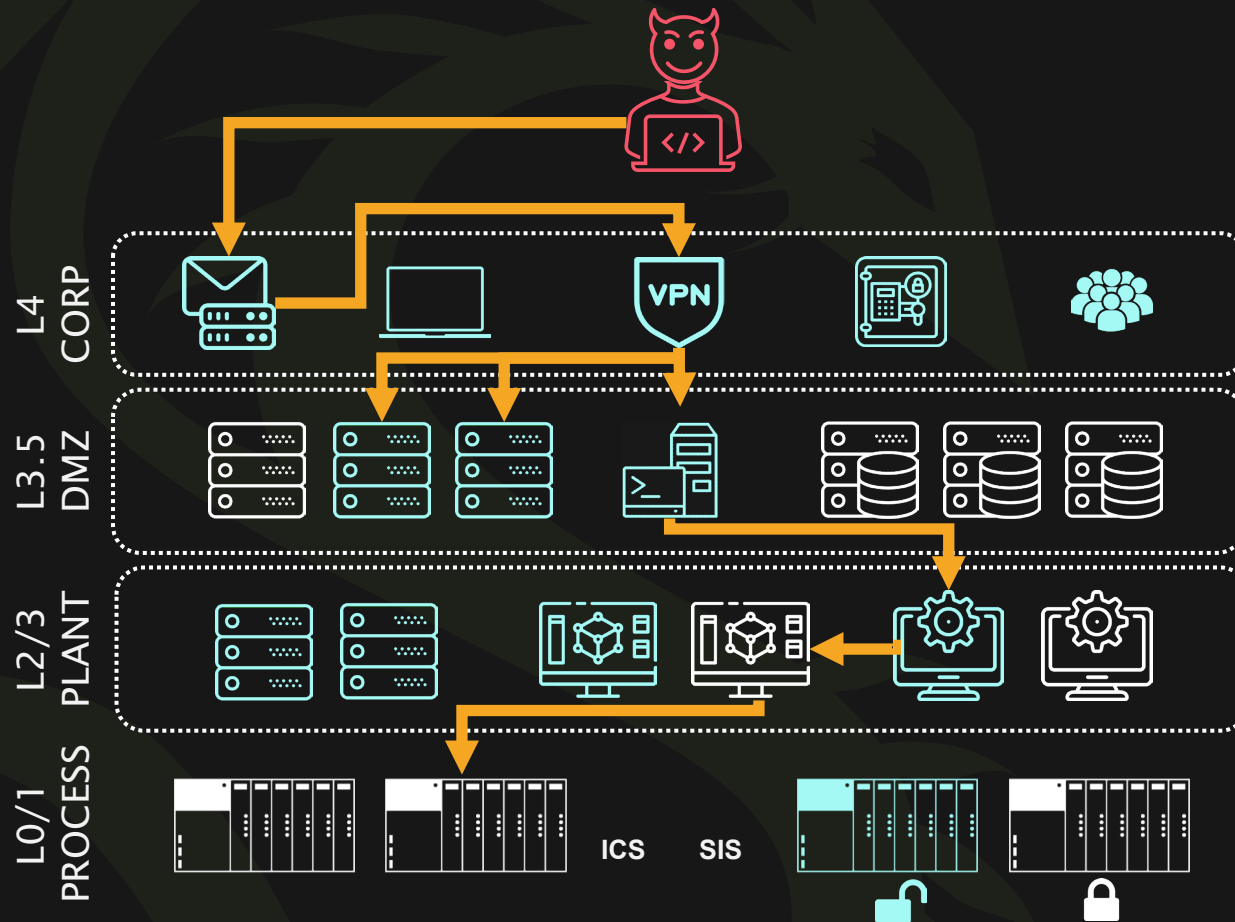
Ransomware

What everyone's talking about

- 10% of ransomware attacks from 2018 – 2020 impacting industrial entities targeted electric utilities
- Ransomware strains have begun adopting OT-aware functionality, including the ability to kill industrial focused computer processes
- Ransomware doesn't have to hit OT to impact OT

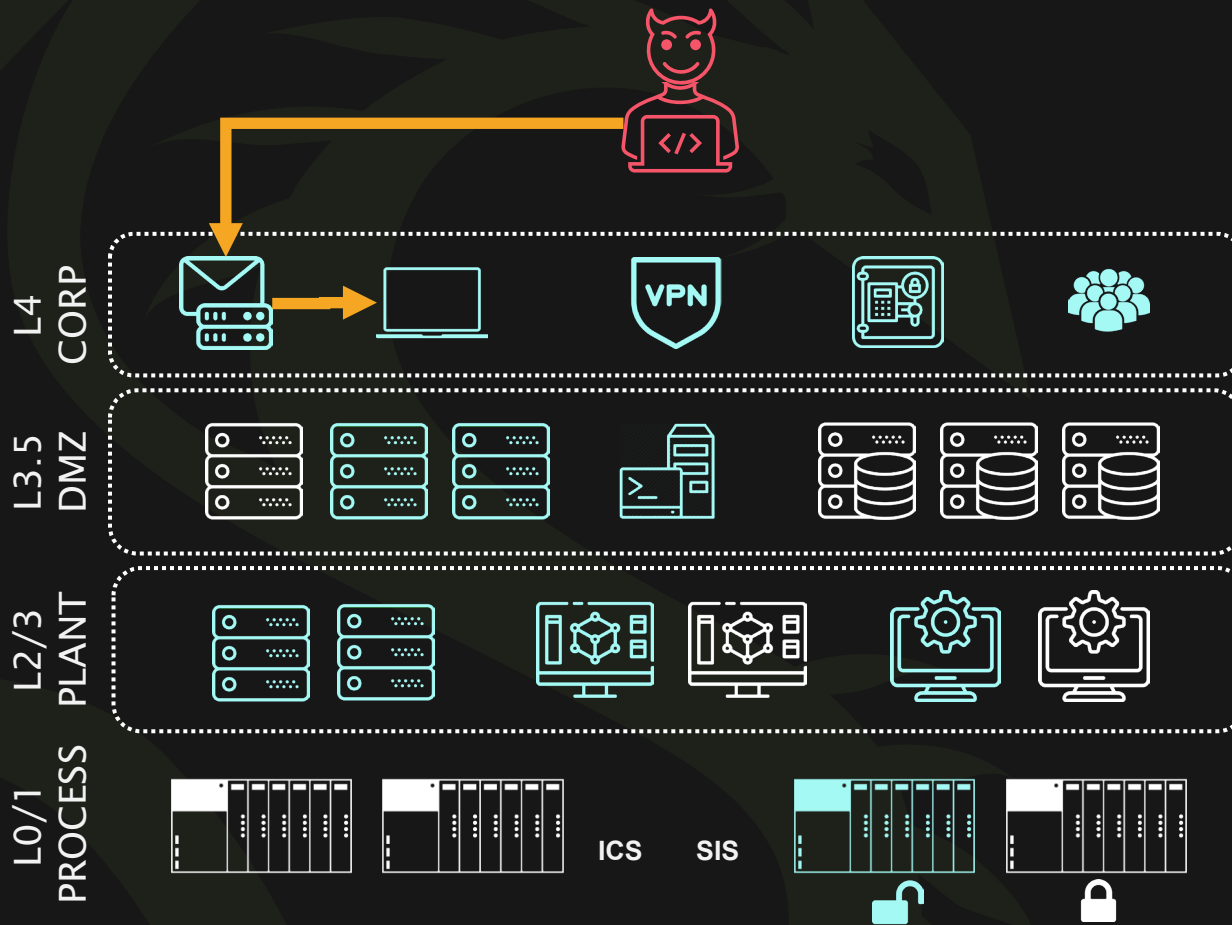


Adversarial Perspective



Adversaries must go through the ICS Cyber Kill Chain to produce specific effects on OT systems/assets.

Adversarial Perspective



Targeting corporate/OOB systems can enable less sophisticated adversaries to effect non-specific effects on operations.



But NERC CIP...

Its Great!

But what are the limitations?

Bulk Electric System

CIP standards are intended to support the reliability of the *bulk* electric not individual utilities

Limited Scope

Low impact generation and transmission and distribution systems aren't subject to CIP requirements

No Threat Management Requirements

While understanding threats helps support CIP compliance, it is not specifically required

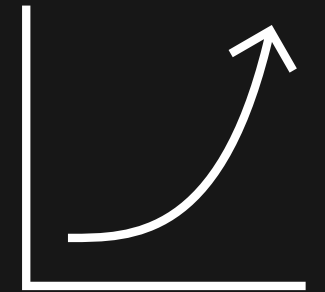
Understanding Industrial Cyber Risk



Are threats decreasing?



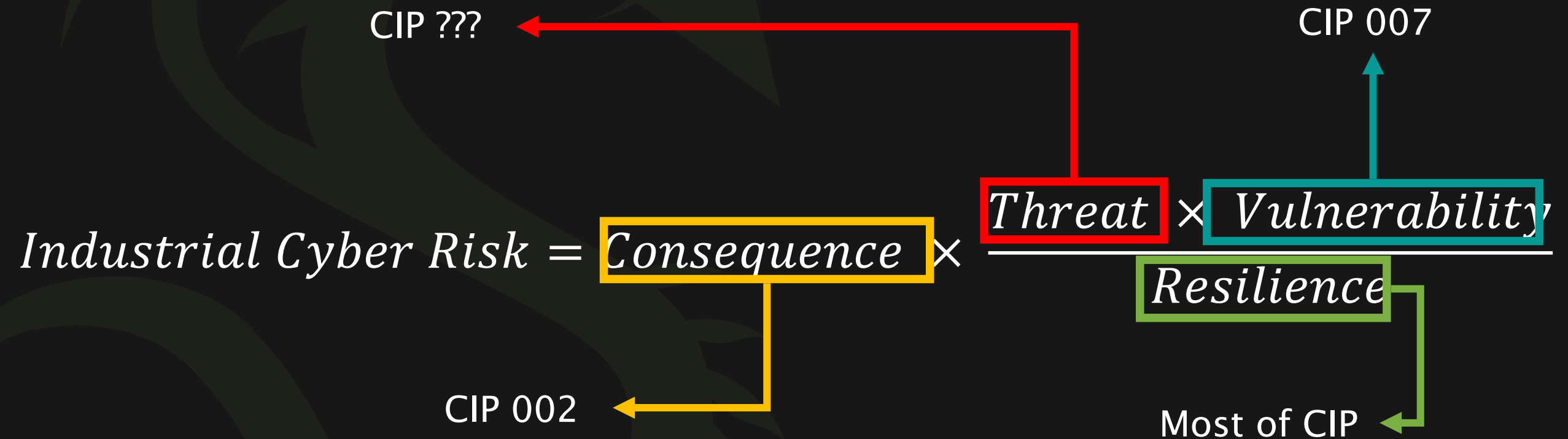
$$\textit{Cyber Risk} = \textit{Consequence} \times \textit{Threat} \times \textit{Vulnerability} =$$



Are vulnerabilities decreasing?



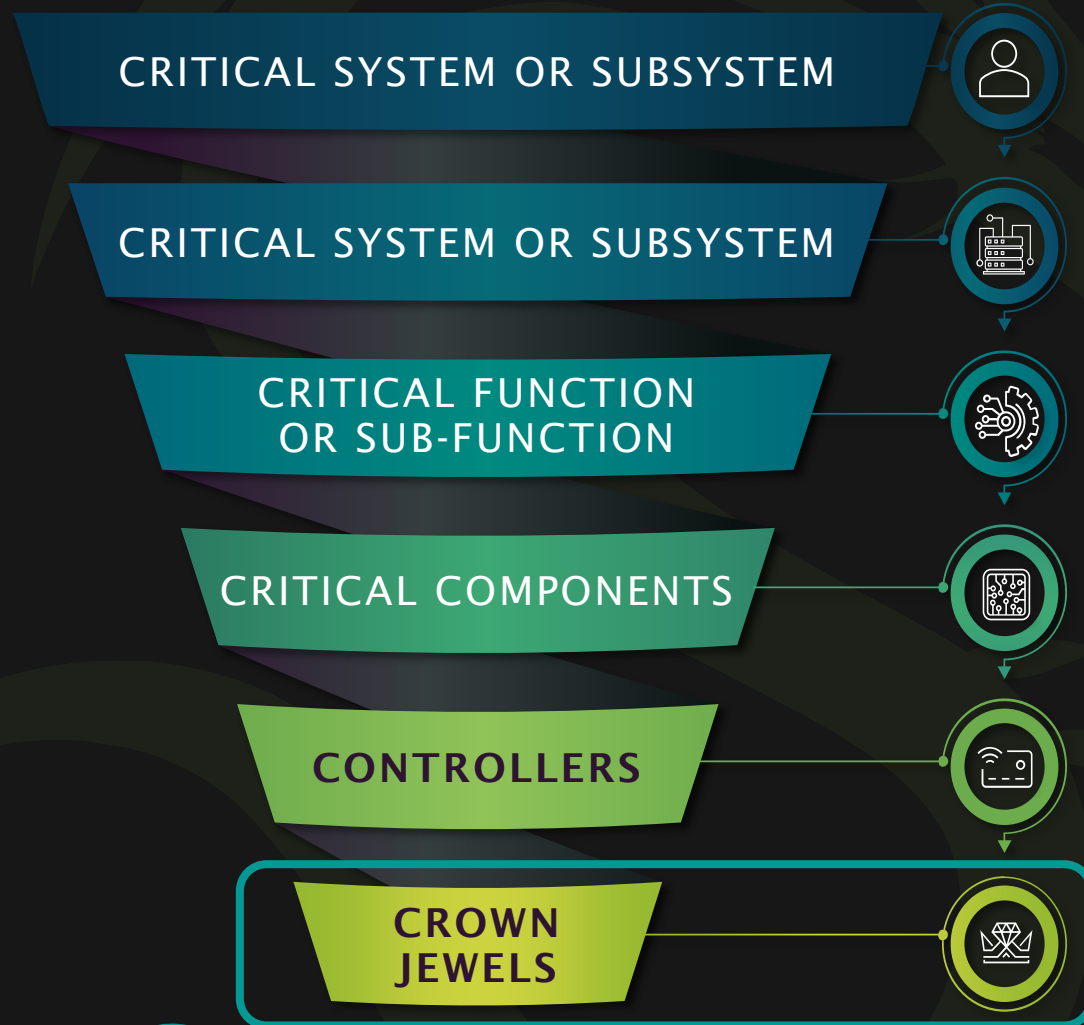
Rethinking Cyber Risk



The background features a dark, moody image of a Ferris wheel, likely the London Eye, with its intricate metal framework visible. Overlaid on this are various abstract, light-colored geometric lines and shapes, including circles, squares, and lines with arrows, suggesting a technical or digital theme.

Recommendations

Know What You're Trying to Protect



- What would happen if we lose view or control of the crown jewels?
- What would happen if an attacker denied us view, control, or safety around the crown jewels?
- What would happen if an attacker manipulated the view, control, safety, or sensors and instruments around the crown jewels?

Gain Situational Awareness

MITRE | ATT&CK[®]

MatricesTacticsTechniquesData SourcesMitigationsGroupsSoftware

GROUPS

Overview

admin@338

Ajax Security Team

ALLANITE

Andariel

Aoqin Dragon

APT-C-36

APT1

APT12

APT16

APT17

APT18

APT19

APT28

APT29

APT3

APT30

APT32

APT33

APT37

APT38

APT39

APT41

Aquatic Panda

Axiom

BackdoorDiplomacy

BITTER

Sandworm Team

Sandworm Team is a destructive threat group that has been attributed to Russia's General Intelligence Directorate (GRU) Main Center for Special Technologies (GTSST) military intelligence. The group has been active since at least 2009, and is known for its sophisticated cyber operations: the 2015 and 2016 attacks against Ukrainian electrical companies and organizations, the 2017 worldwide NotPetya attack, targeting of the 2017 French presidential election, the 2018 Olympic Destroyer attack against the Winter Olympic Games, the 2018 operation for the Prohibition of Chemical Weapons, and attacks against the country of Georgia. Some of these were conducted with the assistance of GRU Unit 26165, which is also known as the FANCY BEAR group.

Associated Group Descriptions

Name
ELECTRUM
Telebots
IRON VIKING
BlackEnergy (Group)
Quedagh
Voodoo Bear

Techniques Used

Domain	ID	Name	Use
Enterprise	T1087	.002 Account Discovery: Domain Account	Sandworm Team used this technique to obtain usernames and email addresses of users in the target organization.
		.003 Account Discovery: Email Account	Sandworm Team used this technique to obtain email addresses of users in the target organization from the M.E.D. group.



DRAGOS

WorldView ICS Threat Intelligence

PROPRIETARY
CONFIDENTIAL

TLP: AMBER For Dragos Customers

THREAT INTELLIGENCE SUMMARY

AA-2022-44: Impacket and CovalentStealer Used in a Compromise of a Industrial Base Organization

04 October 2022

ICS Impact

On 04 October 2022, The United States (U.S.) Government released a joint advisory on a known threat group, Impacket and CovalentStealer, to compromise and exfiltrate sensitive data, respectively, Defense Industrial Base sector organization.¹ In addition to these two tools, China Chopper web shells and remote access tool were also discovered. Dragos tracks three threat groups that have used Impacket and CovalentStealer – ELECTRUM, ALLANITE, and PARISITE.

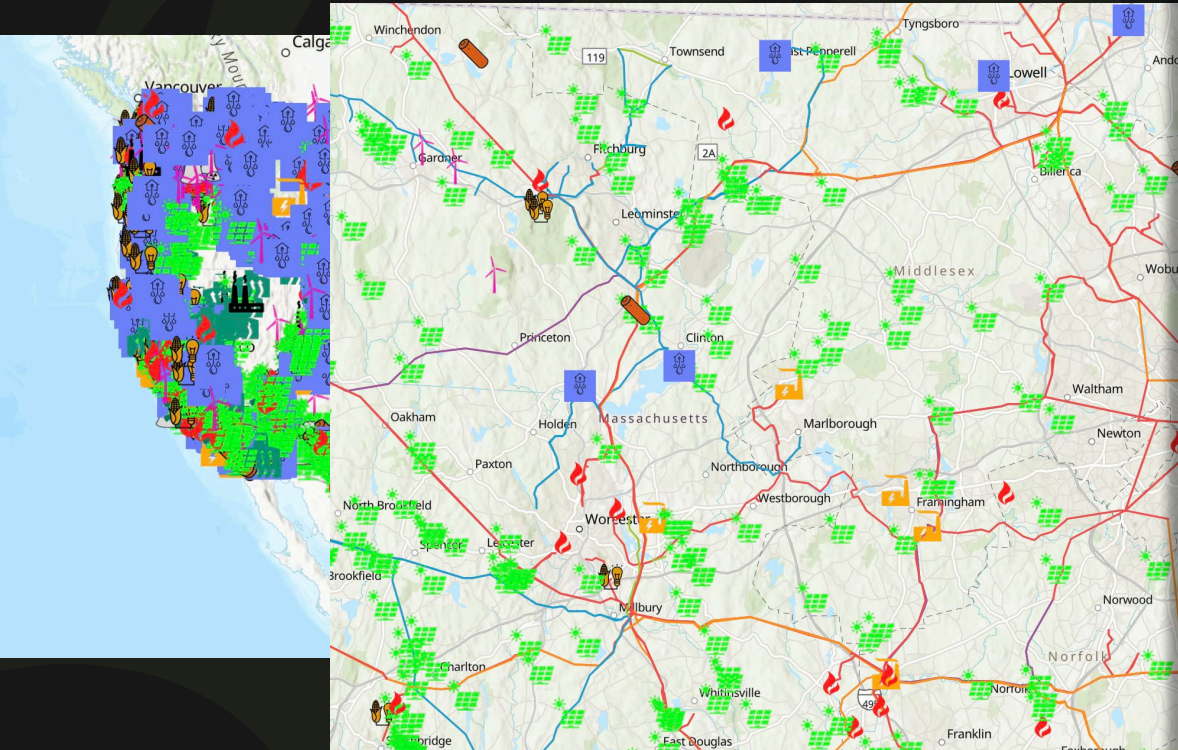
Threat Analysis	Analyst Assessment
Audience	Industrial Control Systems (ICS) Professionals, Managerial Operations Technology (OT) Cybersecurity Operations Professionals, Vulnerability & Risk Management and Information Technology (IT) Professionals (Managers, IT Cybersecurity Operations Professionals, Vulnerability & Risk Management)
Targeted Sector/Industry	Energy – Electric (2211), Government- Defense Industrial Base (9211), Energy – Oil & Gas (2111)
Targeted Region	Worldwide
Threat Group	ELECTRUM, ALLANITE, PARISITE, CHRYSENE
Threat Intelligence Score	A limited threat, risk, or vulnerability requiring an assessment before taking action
ICS Cyber Kill Chain Stage	Stage 1 – Reconnaissance, Targeting, Install/Modify, Control, and Control, Actions on Objectives Stage 2 – Install/Modify ²
MITRE ATT&CK Techniques	See Appendix A for full details

¹ Impacket and Exfiltration Tool Used to Steal Sensitive Information from Defense Industrial Base Organization - DHS/CISA
² This is only for activity related to ELECTRUM's cyber-attack on Ukraine power utility company in early 2022. See report AA-2022-24 for more details.

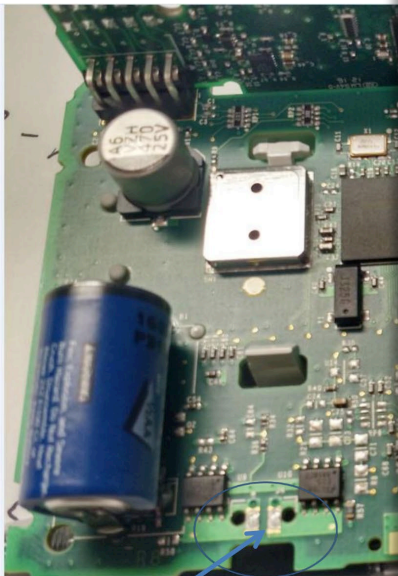
DRAGOS | WorldView Threat Intelligence | Page | 1 | PROPRIETARY AND CONFIDENTIAL

Threat Name		
ELECTRUM		
Threat Category	Threat Subcategory	
Human	Threat Groups	
Intent	Method of Delivery	
Deliberate	Technical	
Threat Description		
Highly sophisticated cyber threats tracked by Dragos that known to target operational technology. Threat groups may overlap with other threat categories.		
Threat Description Notes		
ELECTRUM is responsible for the December 2016 CRASHOVERRIDE attack on a Kiev, Ukraine substation, which blacked out a portion of the city's electricity for about an hour.		
Targeted Asset Types	Geographic Targeting	Motivation
Switchgear and Circuit Breakers	Eastern Europe / Ukraine	Political
ICS Threat Objectives:		
<input checked="" type="checkbox"/> Damage to Property	<input checked="" type="checkbox"/> Loss of Control	<input checked="" type="checkbox"/> Loss of View
<input type="checkbox"/> Denial of Control	<input checked="" type="checkbox"/> Loss of Productivity and Revenue	<input type="checkbox"/> Manipulation of Control
<input type="checkbox"/> Denial of View	<input type="checkbox"/> Loss of Protection	<input type="checkbox"/> Manipulation of View
<input checked="" type="checkbox"/> Loss of Availability	<input checked="" type="checkbox"/> Loss of Safety	<input type="checkbox"/> Theft of Operational Information
Other:		
Enterprise Threat Objectives:		
<input type="checkbox"/> Account Access Removal	<input type="checkbox"/> Defacement	<input type="checkbox"/> Inhibit System Recovery
<input type="checkbox"/> Data Destruction	<input type="checkbox"/> Disk Wipe	<input type="checkbox"/> Network Denial of Service
<input type="checkbox"/> Data Encrypted for Impact	<input type="checkbox"/> Endpoint Denial of Service	<input type="checkbox"/> Resource Hijacking
<input type="checkbox"/> Data Manipulation	<input checked="" type="checkbox"/> Firmware Corruption	<input checked="" type="checkbox"/> Service Stop
<input checked="" type="checkbox"/> System Shutdown / Reboot		
Other:		
MITRE ATT&CK References		Links to Additional Resources
T0865, T0859, T0810, T0853, T0803, T0804, T0805, T0814, T0816, T0806, T0849, T0881, T0855, T0813, T0815, T0827, T0829, T0880, S0001, S0002, S0029, T0819, T0822		https://portal.dragos.com/80threat_groups/CS
Notes		
Dragos associates ELECTRUM with the group dubbed by FinEye as the SANDWORM Advanced Persistent Threat (APT), which was responsible for another Ukrainian power outage in 2015. ELECTRUM previously served as a development group facilitating some of the earlier SANDWORM activity, but the group moved into both a development and operational role in the CRASHOVERRIDE incident.		

Google Yourself – OSINT



The ITRON



To the disconnect solenoid (24 V)

2/16/2017

Security Codes

The meter security codes provide protection for meter register and load profile data. Four levels of security are inherent in the D/T/L Register. The table below describes the level of access to the meter provided by each device security code. Once security codes are programmed and stored in the meter, users are required to logon to the meter with an appropriate password. The user may choose not to use security codes in the meter's program.

D/T/L Register Security Code Levels		
Level	Access Level	Description
Primary/Firmware Download	Read/Write access and firmware download	Access to the meter is unrestricted. All read/write functions are available including all programming options and the ability to download new firmware to the meter. New security codes can be programmed into the meter using the level of access provided by this security code.
Limited Reconfigure	Read/Limited Write access	Provides read and limited write access including the ability to reset demand, change the time in the device, and reconfigure the device. You cannot clear billing data, change display modes, or change security codes.
Secondary	Read-only access plus Demand Reset and Reset Time	Read-only access is provided as well as the ability to reset demand and change the time.
Tertiary	Read-only access	Access to the meter is limited to reading information from the meter. No operation that writes information to the meter is available. This code can be used by other applications that contact the meter.
Previous Security Code	Read-only access	This code is not programmed into the meter; it allows a user to save an alternate password in the software to use for logging on only; can be any security level.

Build an Active Defense

Passive defense is so 2010...

- Standards are great but threats are evolving faster than regulation
- Leverage threat intelligence in conjunction with network visibility to enhance detection and response capabilities
- Establish protective and detective controls through the lens of incident response

Remember that Defense is Doable
Thank you!

Standards Program Update

Gerry Dunbar

NPCC Director Standards and Criteria

November 9, 2022





Overview

- NERC Standards Process Improvement Opportunities
- NERC Standard Activity
 - Distributed Energy Resource Strategy (DER)
 - Variable Energy Resource Strategy (VER)
- NPCC DER/VER Forums.
- NPCC Task Force Criteria Reviews.



Topic – NERC Standards Process Improvement Opportunities

- Standard Development Process
 - Improve Ability to Address Urgent Reliability Needs
 - Maintain Due Process, Openness, and Balance of Interests
- Standards Process Stakeholder Engagement Group (SPSEG)
 - NERC BOT, MRC, NERC Standing Committees (SC, CCC, RSTC, RISC) and NERC Staff
- SPSEG Recommendations for Incremental Process Improvements
 - NERC Rules of Procedure (ROP)
 - NERC Standard Processes Manual --- ROP Appendix 3A
 - NERC Standards Committee to Support Efficiencies



Topic – NERC Standards Process Improvement Opportunities.

- Streamline the Standard Authorization Process (SAR)
 - Revise SAR Form to Drive Clarity on Reliability Issues
 - Create Single Drafting Team for Standard Development Project
 - Eliminate Prescriptive Language
- Streamline Standard Balloting
 - Tiered Comment Period Structure
 - Eliminate Final Ballot Requirement to Confirm Approval
- Review the Registered Ballot Body (RBB)
 - Ten Segments Comprising the RBB



Topic – NERC Standard Activity- DER and VER

- Risk Mitigation Strategy
- Inverter Based Resource Strategy Document
 - PRC-024 Generator Ride Through
 - Numerous Standards Projects Underway
- Distributed Energy Resource Strategy Document
 - NERC System Planning Impacts from Distributed Energy Resources Working Group (SPIDERWG)
 - NERC Reliability Standards Review



Topic – NPCC Activity ---DER/VER Forums

- NPCC Board of Directors Strategic Plan
 - Reliably Integrate DER/VER Resources
 - Promote Communication, Collaboration and Coordination
- 2022 Forum Topics:
 - Electric Vehicle Charging, Building Electrification and Transmission Integration
- NPCC DER/VER Guidance Document
 - Regional guidance and information for voluntary use by NPCC Members and stakeholders.



Topic – NPCC Directories and Criteria

- NPCC More Stringent or Specific Criteria Contained in Directories
 - Applicable to NPCC Full Members
 - Interconnection and Tariff Obligations May Govern Compliance
- Current Reviews:
 - Directory #1 Design and Operation of the BPS
 - Directory #8 System Restoration



Comments/Suggestions/Questions

Gerry Dunbar

NPCC Director Standards and Criteria

GDunbar@NPCC.org

Ruida Shu

NPCC Manager Reliability Standards

RShu@NPCC.org

CIP-008-6 Incident Reporting Study Summary

Cecil Elie
Senior CIP Analyst

Catherine Nakor-Tetteh
CIP Compliance Auditor





Background

- Reliability Standard CIP-008-6 became effective on January 1, 2021, in response to FERC Order No. 848.
- The revised Reliability Standard (CIP-008-6), in part, requires responsible entities to define and report on “attempt(s) to compromise” applicable systems to include EACMS.
- Q3-2021, the ERO Enterprise initiated a CIP-008-6 effectiveness study.





Assessment Approach



- Review of completed compliance monitoring engagements.
- Questionnaire engagement through voluntary mechanism.
- The questionnaires contained 17 questions which focused on:
 - Criteria / Definitions;
 - Organizational / Internal Controls;
 - Training / Tools; and
 - Reporting



Observations of Entities

Most registered entities have processes and internal controls around the detection, review, coordination, and reporting.

Most entities use advanced detection tools.

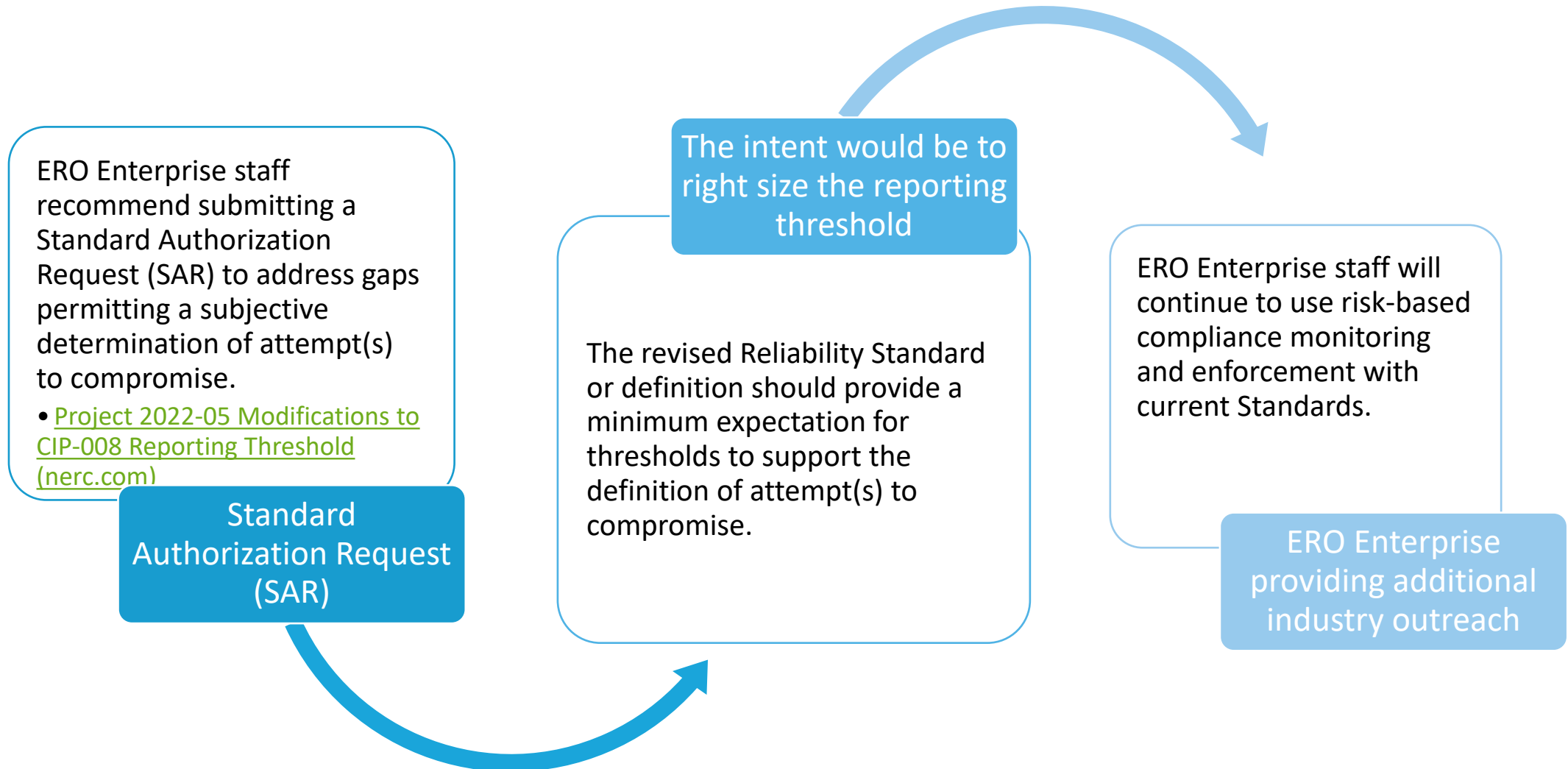
Entities staff is sufficiently trained in incident detection and response.

The current language of the Reliability Standard permits the use of subjective criteria to define attempt(s) to compromise.

Most entity programs include a provision allowing a level of staff discretion.



Recommendations





NORTH

COORDINATING COUNCIL, INC.



Questions

Cecil Elie

celie@npcc.org

Catherine Nakor-Tetteh

ctetteh@npcc.org

PUBLIC