NPCC Compliance Webinar

Welcome

Scott Nied
Assistant Vice-President, Compliance
November 18, 2020

The ERO Golden Circle

Why, How, What

Premise behind the Golden Circle

- The ERO works together as one team and honor each of its roles
- Each Region actively supports ERO Enterprise activities while eliminating unnecessary duplication of work
- Collaborate to develop clear and consistent guidance across the ERO Enterprise
- Share information, knowledge, and resources across the ERO Enterprise
- Develop and share harmonized messages across ERO Enterprise communications
- Support innovation, initiatives, and the sharing of best-practices across the ERO Enterprise

Examples of ERO Aspirations

- The ERO Staff initiatives and behavior are centered around our “why.”

- Our focus and engagement are centered on reliability and security risks. Monitoring engagements are not just about compliance. Is security and reliability sustainable?

- Stakeholders identify with our transformational activities and see value in their monitoring engagement with us.

NPCC - Strategic Reliability Focus Areas

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

Reliable integration of new resources

- A note on the DER Forum
  - Guy Zito, Assistant Vice President - Standards

Enjoy the webinar

- Send your questions in through the chat
- Our experts will vet them

ERO Enterprise Guidance addressing Noncompliance Related to Coronavirus Impacts

- Maintaining Safety of workforce and communities
- Assure Reliability of bulk power system during public health emergency.
- Self-log noncompliance.

May 28 Guidance

- Applies to minimal and moderate risk noncompliance
- Applies to periodic and non-periodic actions.
- Expires March 31, 2021 (* extended)

Spreadsheet and Guidance Location

- https://www.npcc.org/program-areas/compliance/enforcement-and-mitigation

- Scroll to bottom and click on:
  - covid-logging-spreadsheet-template-may-28.xlsx (template)
  - may-29-covid-logging-process.pdf (process)

NPCC COVID-19 Notification Spreadsheet

- Standard, Requirement, Functions
- Start and Possible End Dates.
- Compliance impact details and mitigating controls
- Justification for Exception.

Questions? Email: COVID19_Notifications@npcc.org

Monitoring: COVID-19 Lessons Learned

- Tools: Cisco WebEx meetings and Microsoft Teams allow for same vigorous fashion as those with an onsite aspect
- Creative solutions to sharing evidence such as live video and pre-recorded video over secure web conferences
- If an issue, future travel by a subset to perform a focused on-site review in the safest and quickest manner possible.
- Mindset allows entity flexibility to include more staff in the audit process that otherwise would not have been able to participate in a traditional “onsite” audit
- Future planning and the paradigm of conducting audits. Identifying opportunities for enhancement.
- NPCC annual in-person compliance workshops were also transitioned to webinar format and purposely focused to share the most important messages on compliance and reliability. (330 + 225 + 300? Today = 855!)

Questions

Entity Preparation for Virtual Audits

Jacqueline Jimenez

Manager, Compliance

Virtual Audits

- Due to COVID-19, on-site audits have been transitioned to virtual/remote audits.
- NERC guidance has suspended on-site activity through the end of Q1 2021.
- Virtual audits are conducted as closely as possible to an on-site audit via WebEx.
- Preparation is key to a successful outcome.

Image: https://www.alcumusgroup.com/getattachment/1c65e3ba-65e4-4651-b287-8525790a564e/5-Tips-For-Preparing-For-Your-Remote-Audit

What should I expect?

Image: https://thecustomboxesuk.files.wordpress.com/2017/09/what-to-expect-e1506074802292.jpg

- A virtual audit will typically be the same duration as an on-site audit.
  - If additional time is needed, NPCC will coordinate mutually agreed upon dates to complete the audit.
- A virtual audit will occur during the same week as the previously scheduled on-site audit.
- Pre-audit activities will be the same for a virtual and on-site audit.
- O&P and CIP interviews will occur concurrently.
- A virtual pre-audit cyber inspection, if applicable.

What do I need to make sure I am ready?

- Ensure you are familiar with WebEx prior to your audit to avoid unnecessary delays.
- Confirm audio and internet connections work.
  - NPCC can schedule a test WebEx session before your audit week to test connections, audio, screen sharing.
- Establish how you will caucus – in person, virtually, or teleconference
  - Keep in mind any SMEs participating remotely.

Image: https://www.engageselling.com/blog/be-prepared/

What do I need to make sure I am ready?

- Assign a person to document data requests
  - NPCC will also be documenting data requests
- Be prepared to present any evidence and documents during the interviews.

Image: https://www.gilacountyaz.gov/government/health_and_emergency_services/health_services/images/AreYouPrepared-3.jpg

Virtual Audit Week

- A draft schedule is sent approximately 1 month prior to the audit start.
- Entities have the opportunity to comment and suggest schedule changes if needed.
- O&P and CIP interviews occur concurrently.

© Can Stock Photo

Virtual Audit Week

- The audit begins with opening presentations by NPCC and the Entity.
- Multiple breaks throughout the day will be scheduled to reduce fatigue.
- Constant communications with ATLs
- Daily Summaries via email
- NPCC caucusing via Microsoft Teams
- Flexibility is key!

Image: https://www.istockphoto.com/illustrations/internal-audit?mediatype=illustration&phrase=internal%20audit&sort=mostpopular

Audit Tips

- Be innovative with evidence typically seen in person/on-site
  - "Think outside the box"
  - Control room tours – annotated pictures, live video tour, pre-recorded video tour
- Understand the requirements
- Know what the auditor is looking for
  - Review the Measure of the Requirement and Compliance Assessment Approaches in the RSAW.

Image: https://processors.wiki.ti.com/images/5/5c/Helpful_tips_image.jpg

Audit Tips

- Annotate and analyze the evidence
  - Ensure you identify how and where in the document it supports compliance
  - The more specific and explanatory, the less data requests and follow-up questions
  - Confirm evidence supports your compliance with the requirement.
- Perform mock audits
- Ensure SMEs understand how the evidence submitted supports compliance.

Audit Tips

- Ensure the CIP ERT Level 1 evidence requests, PRC-005 equipment list, BES facilities list are accurate
  - Effects the sampling process
  - Inaccurate lists can cause audit delays and reduce entity's time to prepare evidence for sample sets

Image: http://crocehomeimprovement.com/helpful-tips/

Audit Tips

- Develop relevant compliance narratives that accurately and succinctly speak to the evidence provided and how it supports compliance.
- Organize your evidence appropriately
  - Use naming conventions as per the ERT user guide
  - Folder structure of evidence submittals by Standard then Requirement and Sub-requirement or Requirement Part.

Questions?

jjimenez@npcc.org

2020
Outreach and Trend Sharing

November 18, 2020

Scott Nied – Assistant Vice President, Compliance

A note on FAC-003

Transmission Vegetation Management

- Minimum Vegetation Clearance Distance (MVCD) in R1 and R2

2020 Outreach

- February 14 – Targeted GO/GOP on 2020 Audit schedule
- FAC-008 Survey
- Compliance Bulletins – All stakeholders
  - March 24
  - March 27
  - July 1
- Sept 30, 3rd Quarter – All 2021 Audit entities
- CIP-013 Outreach
- Self-Logger and Self-Reporter Outreach

February 14 Outreach

- Targeted to GO/GOP on 2020 audit schedule
- Trends were shared
- Root causes
- Give # of SR that have come in since then who are audit schedule
- A chance for self-report credit

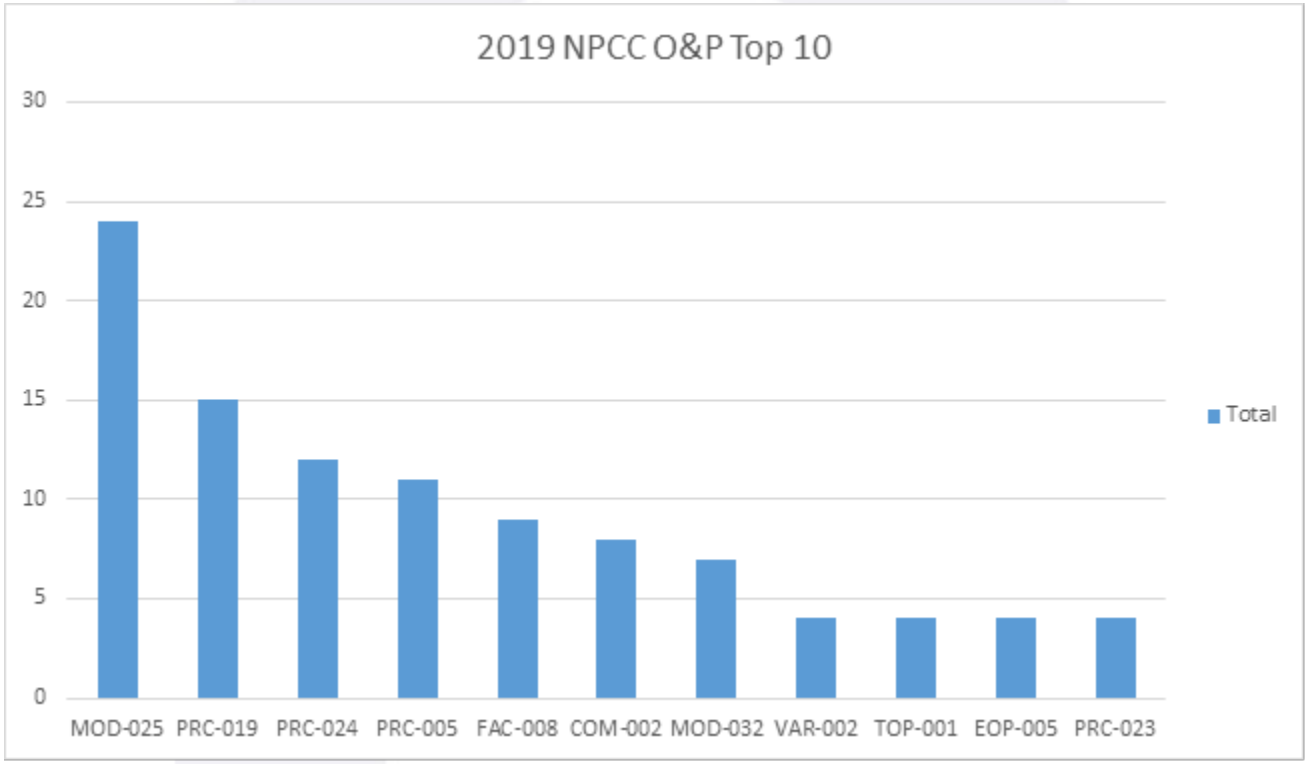
FAC-008 Survey

- February 12, 17 largest TOs in NPCC
- Intent: Your program is paramount to reliability
- NPCC assesses and trends responses
- NPCC acquires global insight to bring to the table with all TOs and GOs

March 24 and 27 Compliance Bulletin

- Similar to Feb 14 email to audited entities
  - O&P Trends
  - Root causes
  - Posted on NPCC website
- CIP-013 outreach explained
  - Separate presentation on this webinar
- FAC-008 survey effort
  - Why?
  - Purpose

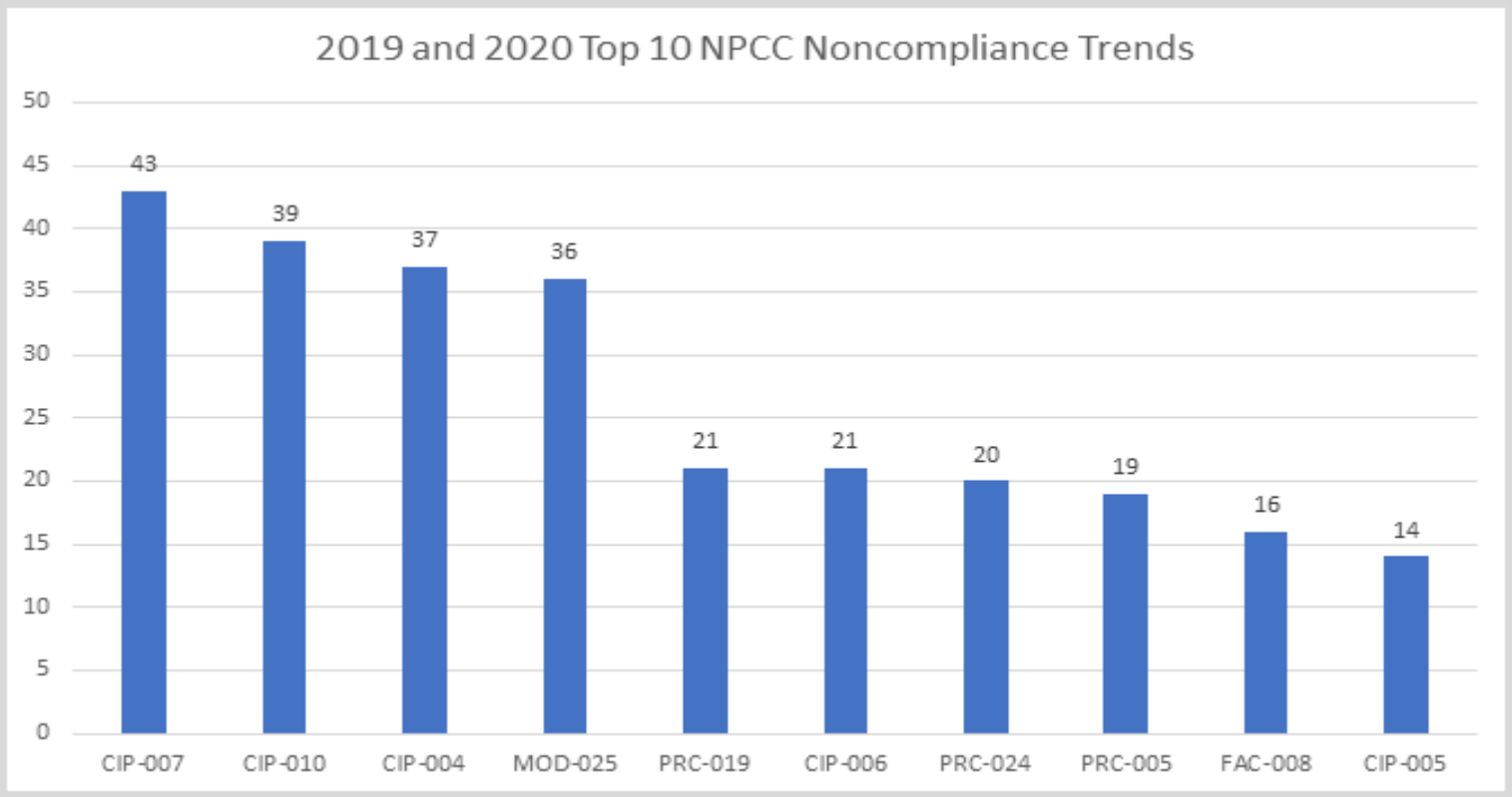
March 2020 O&P Trends



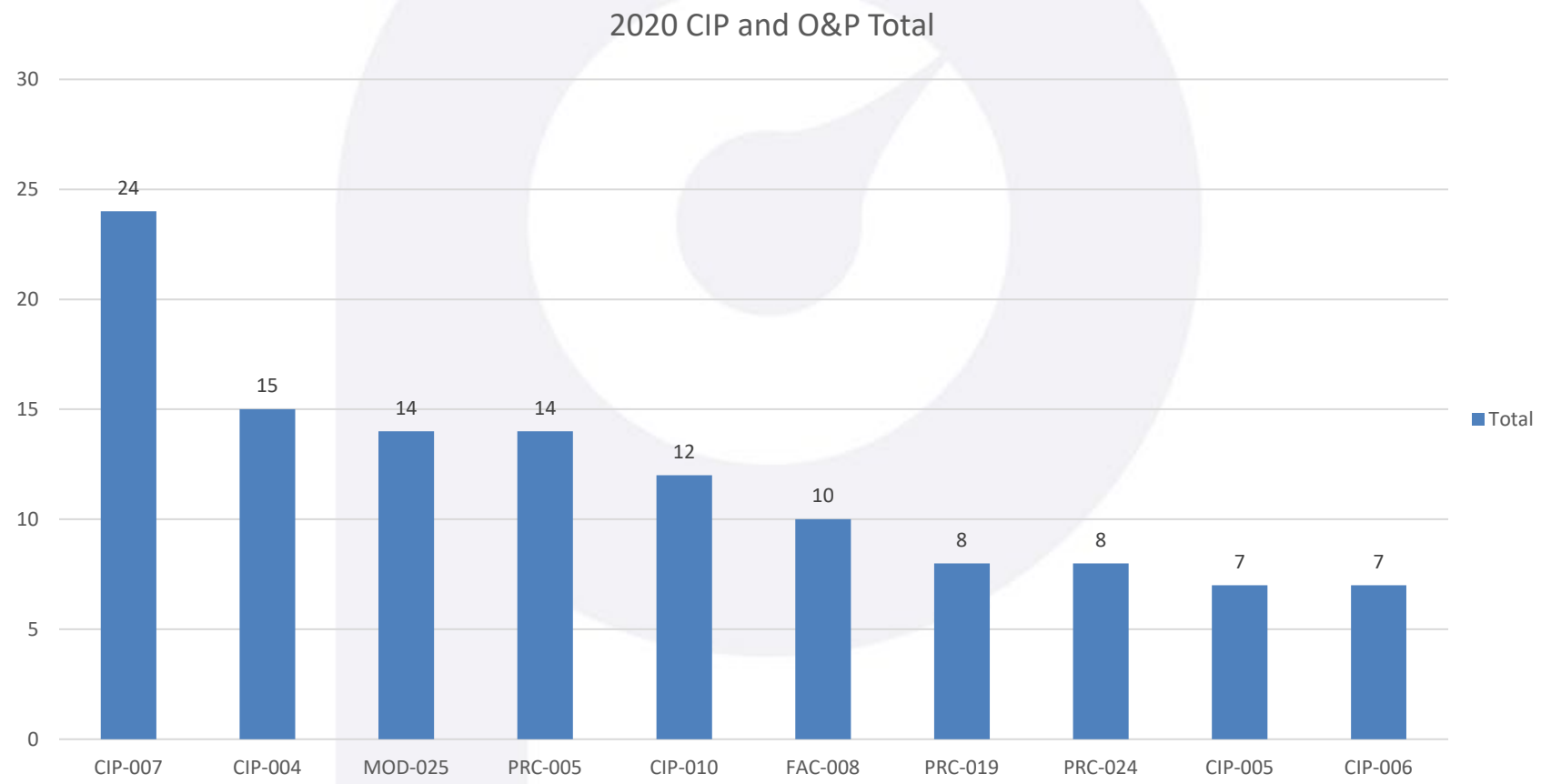
3rd/4th Quarter 2020

- Developed 2021 monitoring schedule
- 9/30/20 - entities on 2021 schedule contacted
- Trends (updated) were explained again

2019/2020 CIP and O&P Total



2020 CIP and O&P Total



What is the deliverable?

- Increased entity awareness
- Earlier discovery by the entity
- Mitigation starts earlier
- BES risk is reduced/eliminated

Why are FAC-008 Facility Ratings important?

They are the main component in the determination of accurate System Operating Limits

Without accurate Facility Ratings, accurate real-time situational awareness is not accomplished and planning models are inaccurate.

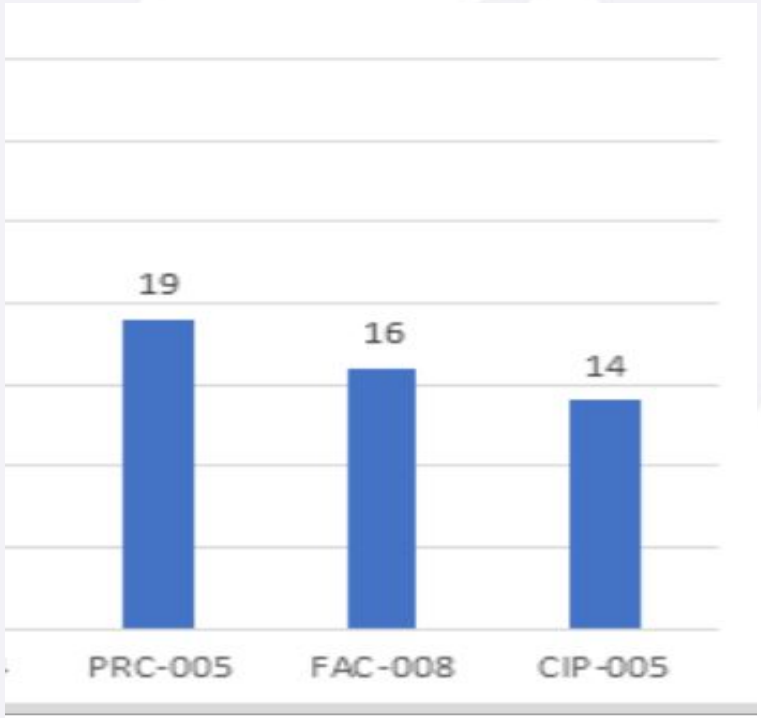
- Interface MW Flow
- Transient Stability
- Voltage Stability
- System Voltage Limits
- Interconnection Reliability Operating Limits

ERO Trends and Perceptions

- NERC Board of Trustees, ERO CMEP Implementation Plan
- SERC started field visits in 2018
- FAC-008 Violations
  - Self Reports
  - Audit Discoveries
    - Reasons: Database issues, Changes in Field, Change Management
    - Most Limiting Series Component not respected
- NPCC Discoveries, Last 3 years

  Self-report: 27 Requirements, 18 entities; Onsite Audit: 1; Offsite Audit: 1

2019/20 FAC-008




Area of Focus
ERO Enterprise Outreach
CMEP Staff Coordination
Coordination with NATF
Coordination with FERC
CCC Facility Ratings TF
CMEP Practice Guide
Facility Ratings

FAC-008 NPCC Actions Toward Mitigating the Risk

- Have spread greater awareness over the past 2 years
  - Socialization began in 2018: Compliance Committee, Workshops, Webinars
- Diagnosis: Not a pandemic
- March 2020 Data Gathering via Survey
- NPCC Compliance Bulletin
- Audits, Substation Visits
- Assessments of Controls – Sustainable?
- Entity example from Ben Eng later in this webinar

Thank you

- My name is Scott

- I can be reached at snied@npcc.org
- Or call/text me at 917-693-1227
- Blind phone calls >>> take your chance.

Self-Logging, Self-Reporting, and Internal Compliance Programs

Damase Hebert and Jason Wang

November 18, 2020

NPCC Fall Workshop

Overview of Presentation

- Self-reporting
- Self-logging
- Internal Compiance Programs

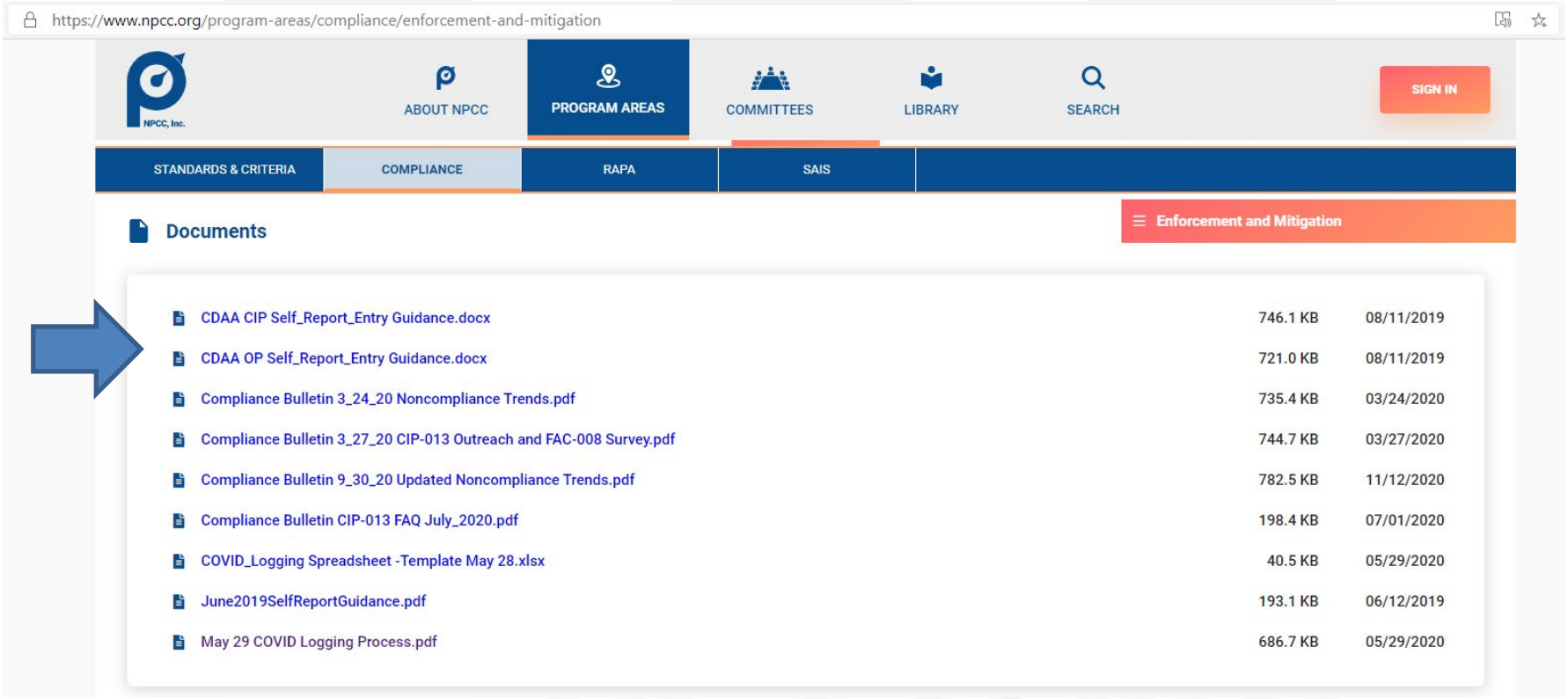
Self-Reports

Purpose: To communicate a mutual understanding of the facts and circumstances, risk, and mitigation surrounding a noncompliance.

Inherently, comprehensive Self-Reports result in less questions and evidences a stronger internal compliance program.

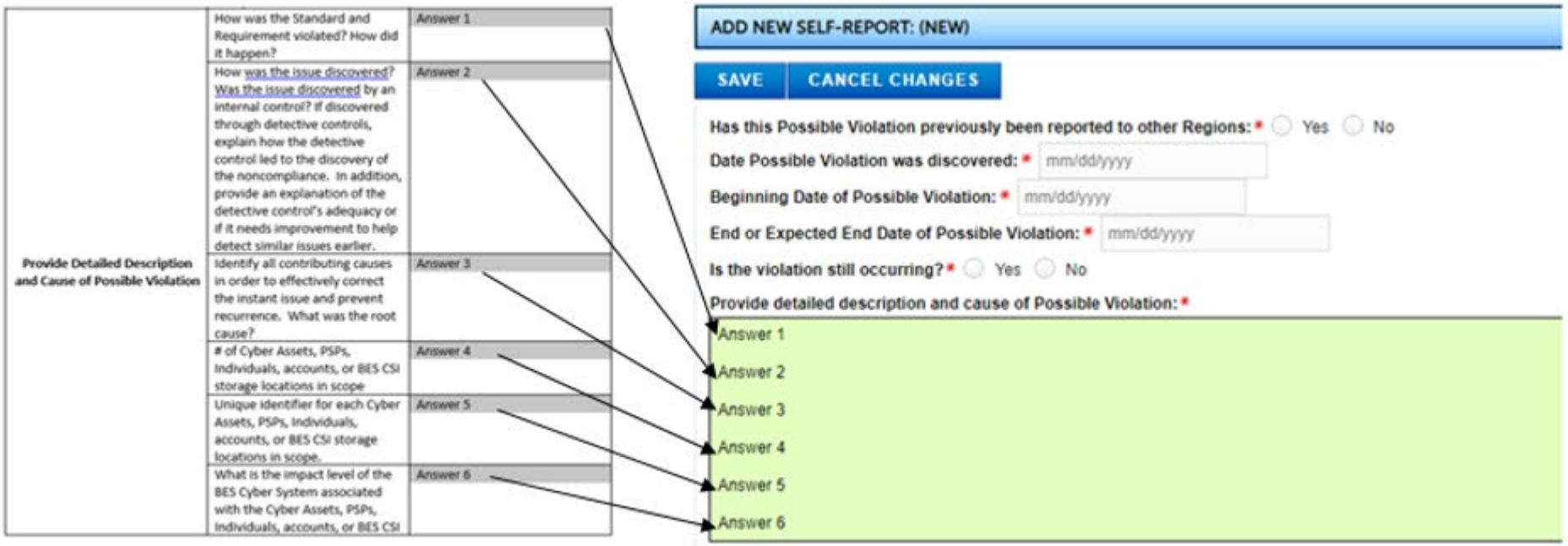
CIP & O&P Self Report Guides

https://www.npcc.org/program-areas/compliance/enforcement-and-mitigation



CIP & O&P Self Report Guides

- Copy and paste each answer field into the appropriate self-report section.



Self-Logging

- Basics
  - Must be pre-qualified
  - Presumption of qualification for compliance exception treatment
  - Minimal Risk Noncompliance only*
- Enhancements
  - Draft posted CMEP ROP revisions
  - ICP Review Report

Internal Compliance Programs

- Program should be designed to prevent and detect noncompliance
- Effective ICPs have executive and management involvement
- NPCC examined seven components of an ICP

Summary of NPCC's ICP Evaluation

- NPCC evaluated the documented ICP using the 36 questions.
- 0 or 1 - ICP did not address the question or did not describe it fully, clearly, or provide enough detail
- 2 - ICP fully, clearly, and satisfactorily documented the concept identified by the question
- 3 - Better practice element

- Average Entity Score of all ICPs Reviewed to Date: 1.51

ICP - Organizational Structure/Resources

- Clear roles and organizational structure
  - For compliance
  - For oversight of compliance
  - For senior management/executives
- Independent Compliance Department
- Sufficient compliance resources
- Access to executives

Better Practice Element – Organizational Structure/Resources

- Structure and Reporting at one large entity includes:
  - Compliance department
  - Steering committee with senior management/executive
  - Bi-monthly reports to steering committee
  - Regular meetings

ICP – Compliance Awareness/Training

- ICP dissemination
- How staff are made aware of compliance responsibilities
- Formally documented training
- Methods to combat complacency
- Participation in peer groups, NERC/Regional Entity Committees, etc.

Better Practice Elements – Compliance Awareness/Training

- Detailed identification of requirements and departments / personnel responsible for compliance
- Combination of specific training and frequent communication
- Combination of self-evaluation of internal controls, multiple methods of communication regarding all self-assessments, noncompliance, and near-misses.

ICP – Continuous Improvement and Self-Assessments

- Management Oversight of implementation/effectiveness
- Self-Assessments of ICP performance
- Self-Assessments of compliance
  - Mock audits, etc.
- Trends
- Effectiveness assessments

Better Practice Elements – Continuous Improvement and Self-Assessments

- Risk Based approach for Self-Assessment and/or internal auditing.
- Key Performance Indicators to identify violations, understand root causes, evaluate ICP
- Annual RSAW completion
- Annual internal audits and random spot checks.

ICP – Identifying Noncompliance

- Compliance whistleblowing procedure/process
- Confidential means of reporting violations
- Review of suspected compliance issues
- Provisions for disciplinary actions
- How facts that do amount to noncompliance are addressed

Better Practice Elements – Identifying Noncompliance

- Simple form and clear workflow for reporting noncompliance.

ICP – Assessing Noncompliance

- Process to assess risk of noncompliance
- Process to communicate risk of noncompliance

Better Practice Elements – Assessing Noncompliance

- Detailed risk review includes the nature of the event, the duration of the issue, system impact. and the repeat nature of the issue.

ICP – Correcting Noncompliance

- Process to ensure mitigation and prevention of future noncompliance
- Process to identify root causes

Better Practice Elements – Correcting Noncompliance

- Monthly report of mitigations items

ICP – Internal Controls

- Documented internal controls to mitigate risk of noncompliance
- Internal controls to detect drift from compliance

Questions?

- For Questions, please contact enforcement@npcc.org

FAC-008 Facility Ratings

November 18, 2020

Ben Eng – *Manager, Entity Risk Assessment (ERA), Compliance*

2020 Activity

Outreach and Trend Sharing presentation – Scott Nied

- FAC-008 Survey
- Compliance Bulletins
  - March 24
  - March 27
- Trends
  - Increased entity awareness
  - Earlier discovery by the entity
  - Mitigation starts earlier
  - BES risk is reduced/eliminated

Why are FAC-008 Facility Ratings important?

They are the main component in the determination of accurate System Operating Limits

Without accurate Facility Ratings, accurate real-time situational awareness is not accomplished, and planning models are inaccurate.

- Interface MW Flow
- Transient Stability
- Voltage Stability
- System Voltage Limits
- Interconnection Reliability Operating Limits

2020 Activity

NPCC Outreach for FAC-008

- 2020 Spring Virtual Compliance Workshop
- 2020 July Webinar
  - Sample Controls questions
  - Sample Process Flow Diagram for R3, R6, R8
  - References to additional ERO Guidance
    - Standards Application Guide FAC-008-3, March 21, 2017
    - CMEP Practice Guide, Evaluation of Facility Ratings and System Operating Limits, June 17, 2020
- 2020 Fall Virtual Compliance Workshop
  - Recap the guidance provided by ERO
  - Demonstrate how one entity approached the FAC-008 concerns
  - Inform industry of better practices and benefits to reliability

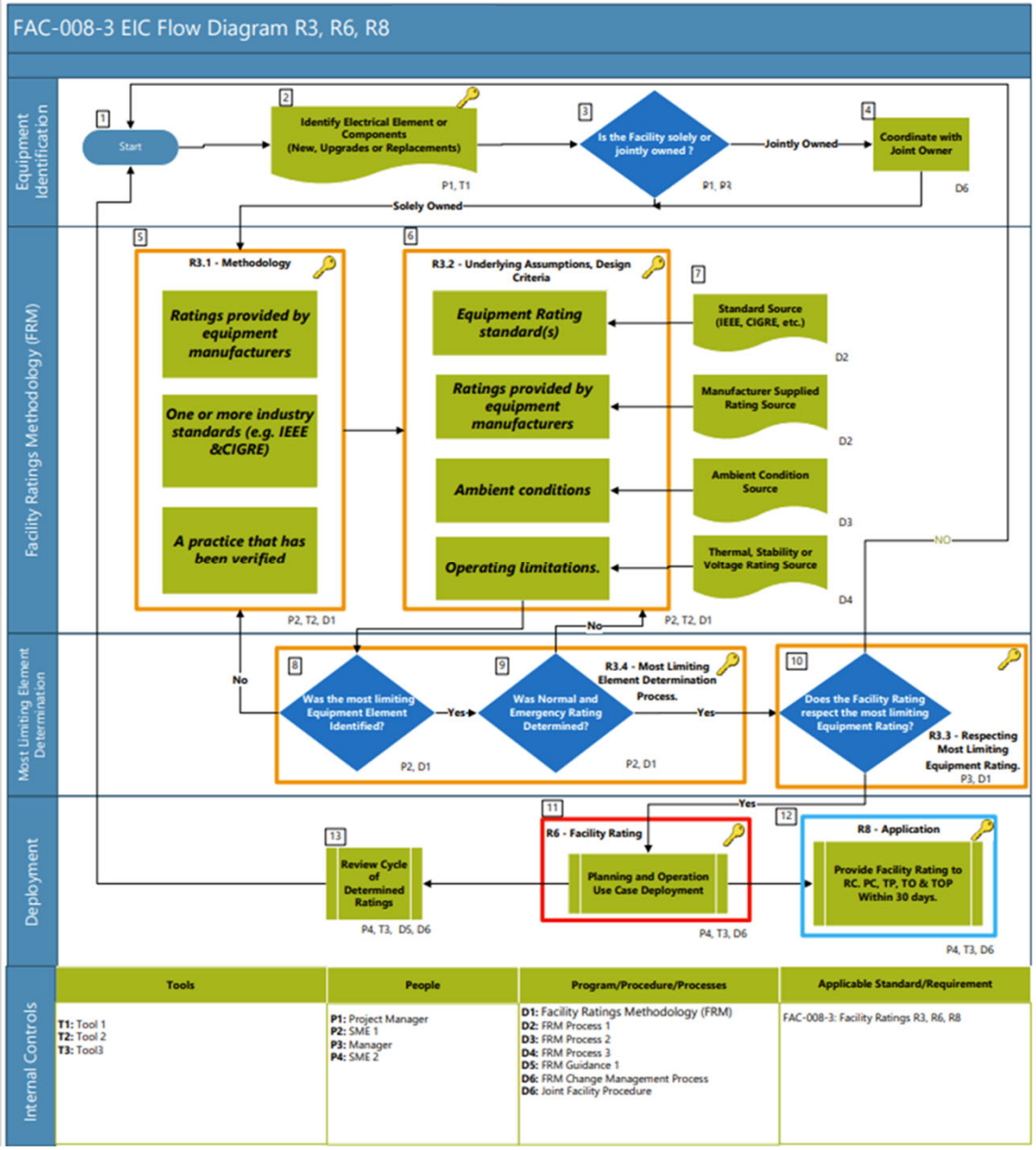
NPCC Sample FAC-008 Controls Questions

Standard	Req.	Control Question.
FAC-008		Does a Facility Rating discrepancy exist between Real-time models (e.g., State Estimator and RTCA), models used for Operational Planning Analysis, and models used in the Short-Term and Long-Term Transmission Planning Horizon? If so, why are the Facility Rating values different?
FAC-008		When a Facility Rating used in the Applications listed above is not the same as that supplied by the Facility Owner, why does that difference exist?
FAC-008		Does the Facility Rating, based on how the Facility is defined in the Facility Ratings methodology, accurately reflect the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility?
FAC-008		Is the Facility rated using a temperature adjusted rating or seasonal ambient temperature rating?
FAC-008		Is the Facility Rating different in EMS due to a nodal operations model vs. a bus line planning model?
FAC-008	R6	Identification of each BES Facility and its Facility Rating is consistent with FRM
FAC-008	R6	Identification of all equipment comprising the Facility
FAC-008	R6	Ratings of all the equipment comprising a Facility are consistent with FRM
FAC-008	R6	Identification of the Most Limiting Series Element (and if applicable, the next Most Limiting Series Element) □ For each owner and each joint owner □ Identification of Normal and Emergency Ratings, as appropriate
FAC-008	R6	Comparison of Facility Ratings between Facility Rating database and: □ Planning models □ EMS/SCADA (tools used to alarm and perform RTCA) □ One-lines and/or design drawings □ Actual field equipment
FAC-008		What tools do you use to track and update your Equipment and Facility Ratings in your Facility Ratings database?
FAC-008		How often do you conduct substation walkdowns to ensure what's in the field matches system one-lines and/or design drawings?
FAC-008		Do you perform an independent review of ratings for all equipment for correctness in the Facility Rating database to ensure the Equipment Ratings are consistent with the FRM?
FAC-008		What is your process following an acquisition or merger to incorporate the new equipment into the Facility Rating database?
FAC-008		What is the Asset Change Management process following a change of equipment in the field, for either a scheduled project or unplanned/emergency

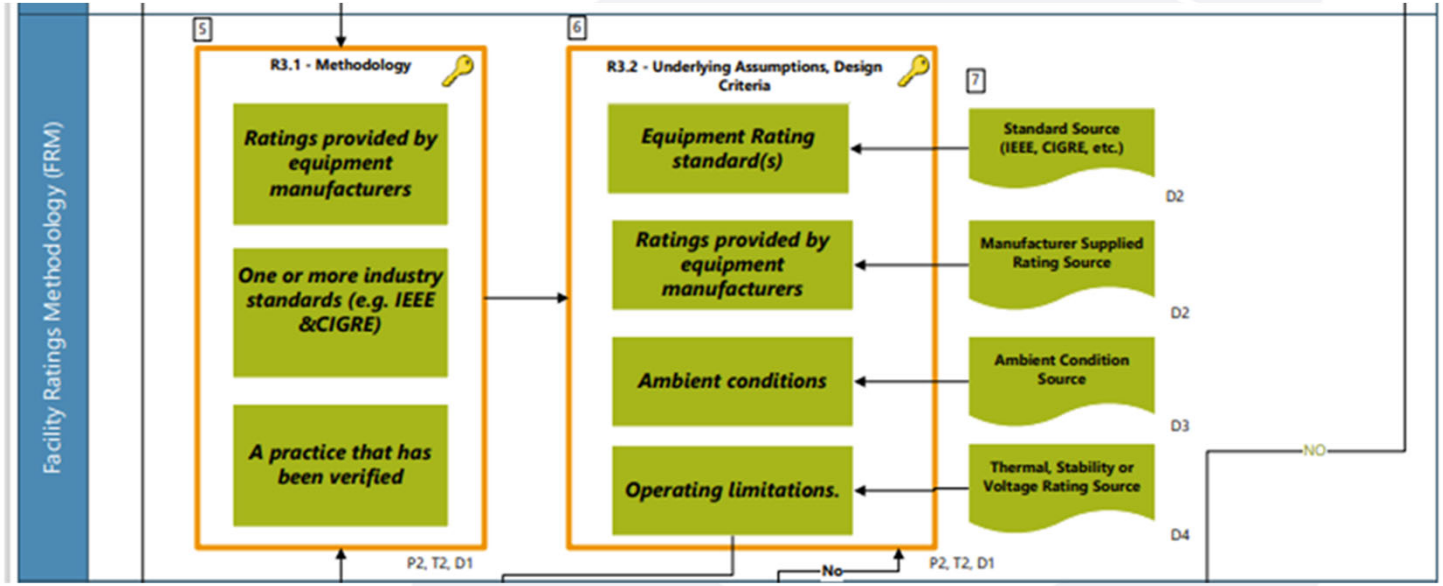
Sheet1

Evaluations of Internal Controls (EIC)

- ACME_EOP-005-3 R1-11_EICworkpaper_annotated.pdf
- draft_FAC-008-3 EIC Process Flow Diagram R3 R6 R8.pdf
- NPCC_sample_FAC-008_EIC_ControlQuestions.xlsx
- ppt_NPCC_FAC008_EIC_ERA_Webpage_071420.pdf



Closer look at suggested NPCC proposed Process Flow



Internal Controls

Tools	People	Program/Procedure/Processes	Applicable Standard/Requirement
T1: Tool 1 **T2:** Tool 2 **T3:** Tool3	**P1:** Project Manager **P2:** SME 1 **P3:** Manager **P4:** SME 2	**D1:** Facility Ratings Methodology (FRM) **D2:** FRM Process 1 **D3:** FRM Process 2 **D4:** FRM Process 3 **D5:** FRM Guidance 1 **D6:** FRM Change Management Process **D6:** Joint Facility Procedure	FAC-008-3: Facility Ratings R3, R6, R8

Submittal from VTransco

- Explanatory Cover Letter
- Existing Controls
- Self-Assessment
- Improvements to Existing Controls (future state)
- Process Flow Diagrams & Supporting Docs

Explanatory Cover Letter

VELCO FAC-008 Evaluation of Internal Controls (EIC)

In going through this exercise of putting this all together, our process included:

- Reviewing our current state
- Identifying GAPS in our current state (self audit)
- Creating a process flow that is that basis for a new process to be followed that will include strong controls in order to meet compliance with the standard

I believe that is ultimately the overall goal of what your team performs.

What I have included in this submittal is the following:

- **1 PRESENT – EP-1 200529_FJH_EJM.pdf** – this is the current methodology for determining facility ratings
- **1 PRESENT – EP-16 – Engineering NX9 Procedure.docx** – this is a procedure that provides guidance in identifying NX-9 applicability when making changes in our transmission system
- **1 PRESENT – EP-16-A1 – Engineering NX9 Checklist.docx** – this is a checklist to follow for updating, and socializing the NX-9 documentation
- **1 PRESENT – EP-16-A1 – Engineering NX9 Process Map.pdf** – which illustrates the work flow and critical path NX9 entry dates for planned work
- **2 SELF AUDIT – VELCO FAC-008 Large Capital Process.pdf** – illustrates the current work flow for large capital projects and identifies areas that are potential gaps and areas where controls would strengthen the process
- **2 SELF AUDIT – VELCO FAC-008 Level I_II_Un Planned Process.pdf** – illustrates the current work flow for level 1, 2 and unplanned work and identifies areas that are potential gaps and areas where controls would strengthen the process
- **3 IN PROGRESS – VELCO FAC-008 Large Capital Process.pdf** – illustrates the updated work flow for large capital projects showing controls including CATSWeb tasks, reviews and notifications that are auto generated and Engineering Procedures (EP), checklists and sign-offs
- **3 IN PROGRESS – VELCO FAC-008 Level I_II_Un Planned Process.pdf** – illustrates the updated work flow for level 1, 2 and unplanned work showing controls including CATSWeb tasks, reviews and notifications that are auto generated and Engineering Procedures (EP), checklists and sign-offs

Explanatory Cover Letter (cont'd)

We wanted to include our current state as that is still how we are doing our facility ratings work. However, we are in the process of adding a process to CATSWeb to include the identified controls, but it is still being created. We wanted to include this piece as it is ultimately our end goal. As other areas are identified where we can strengthen controls, we will work on getting them into the creation of this new process.

Please let us know if you have any questions.

Description of Procedures

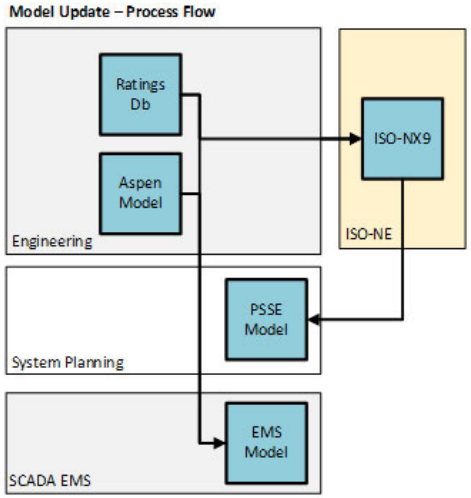
VELCO RATINGS PROCEDURE: EP-1 **Main Document**

EQUIPMENT RATINGS METHODOLOGIES **REV9, 180615**

Description of Procedural Control

Engineering Procedure: NX9 Procedure **EP-16**

Data submitted to NX9 is utilized in three VELCO Models:



- Engineering - Thermal Ratings Database
- Engineering - Aspen Short Circuit Model
- System Planning – PSSE Model
- SCADA EMS – Contingency Model

ISO-NE updates the PSS/e model automatically via NX9. There is some equipment which System Planning must manually check such as shunt devices, STATCOM, SVC, Highgate HVDC, etc.

EMS updates the EMS model upon notifications from engineering via the SMR process.

ROLES AND REPONSIBILITIES

Project Engineer - Project Subject Matter Expert (SME) responsible for managing the project from the scoping phase to project close out. The Project Engineer is responsible for gathering all NX9 data entry materials to be communicated to the VELCO NX9

Description of Control - checklist

	Engineering Procedure	EP-16-A1	
VT TRANSCO VELCO VETCO		Department:	Engineering
	NX9 Checklist	Date Published:	7/2/18
		Current Revision:	Rev 0

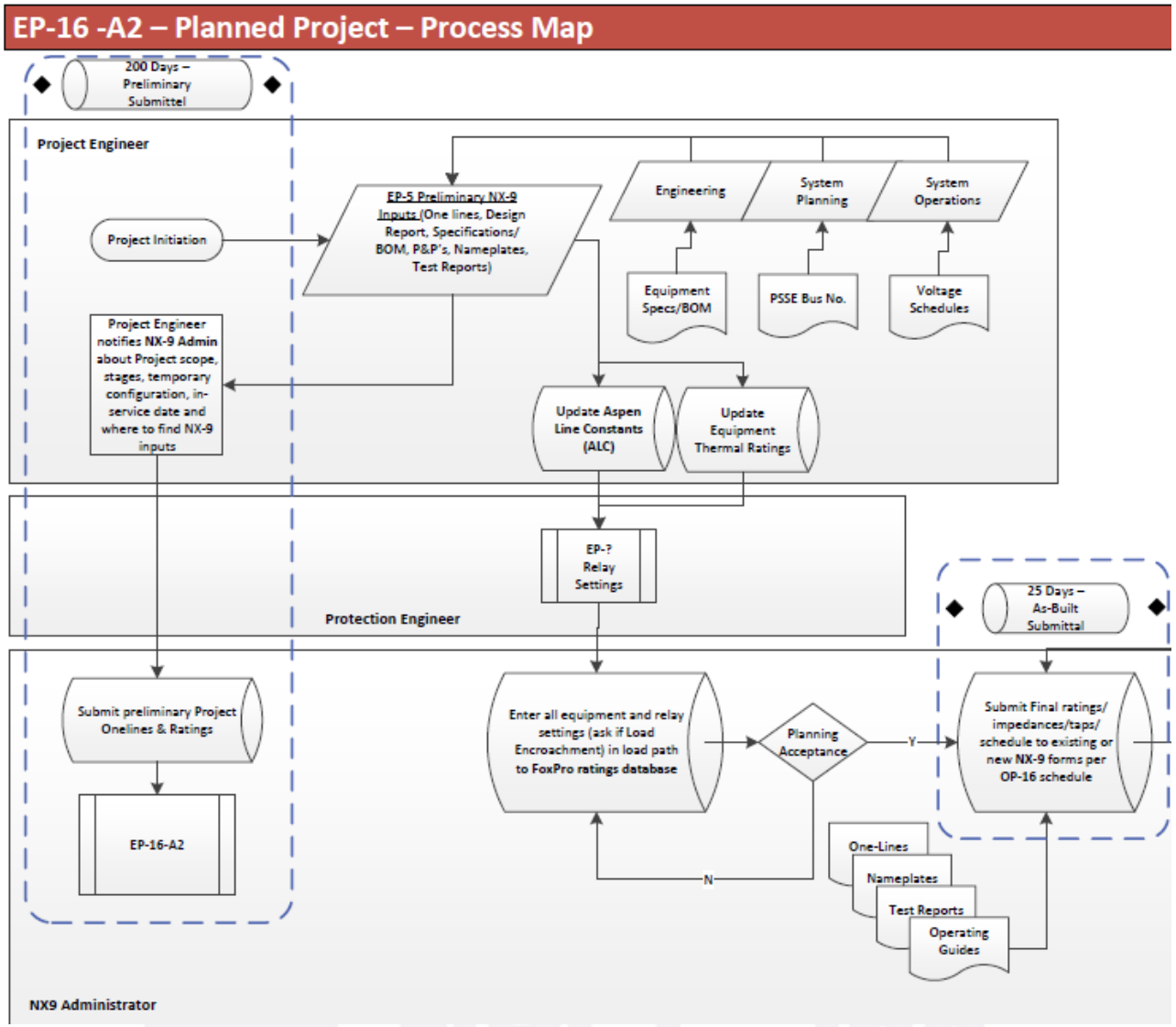
OBJECTIVE

This checklist systematically instructs the NX9 administrator and the action required to update, socialize and archive NX9 documentation.

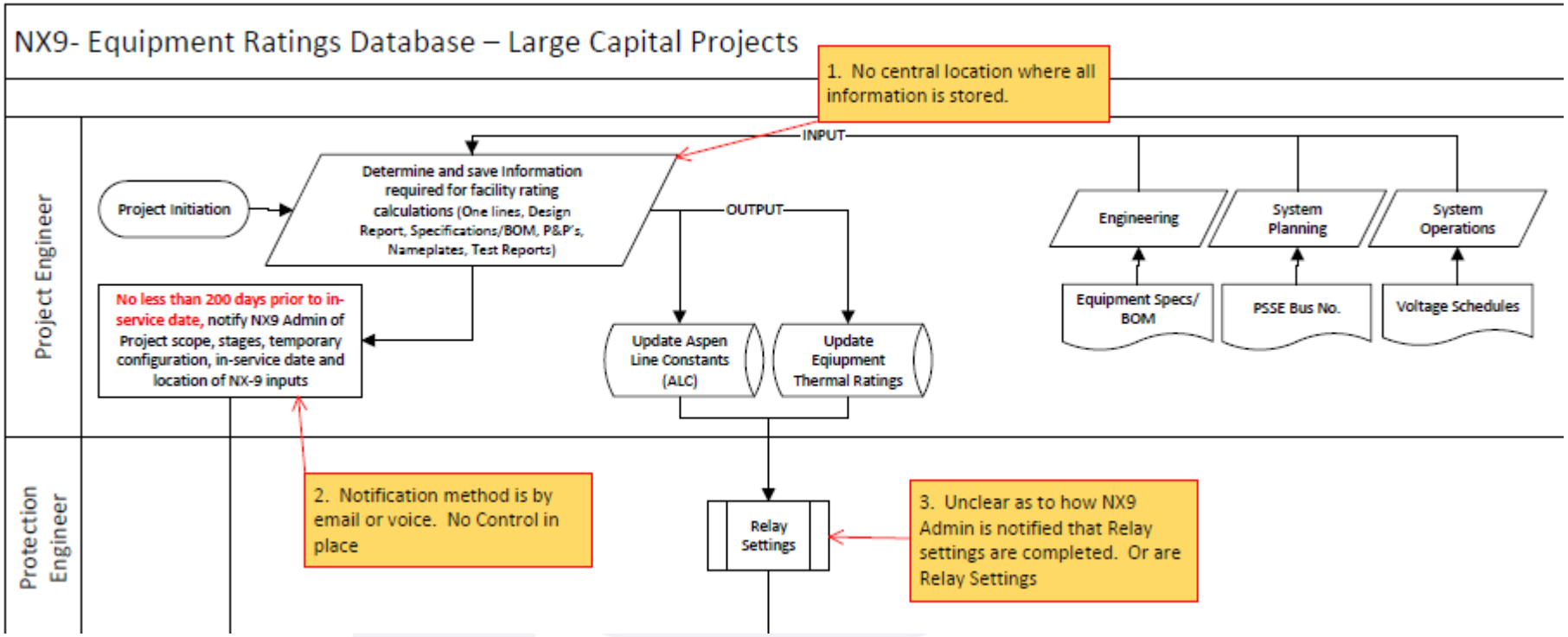
Project:_____ Date:_____ Name:_____

NX9 Administrator Task	Complete (Initials)
VELCO Internal Notification via CatsWeb or Email: • **System Planning**: [redacted] • **System Operations**: [redacted] • **Engineering :** [redacted] • **SCADA EMS:** [redacted]@velco.com	
Post One-line(s)to NX9	
Post Transformer Nameplate	
Post Transformer Test Report	
Develop Adjusted Ambient Thermal Ratings Curves for New Line/Transformer (inc. other limiters) • Engcom\Ratings\docs\Xfrs • Link on Ops Interact Ratings page • Change hard copy in control center	

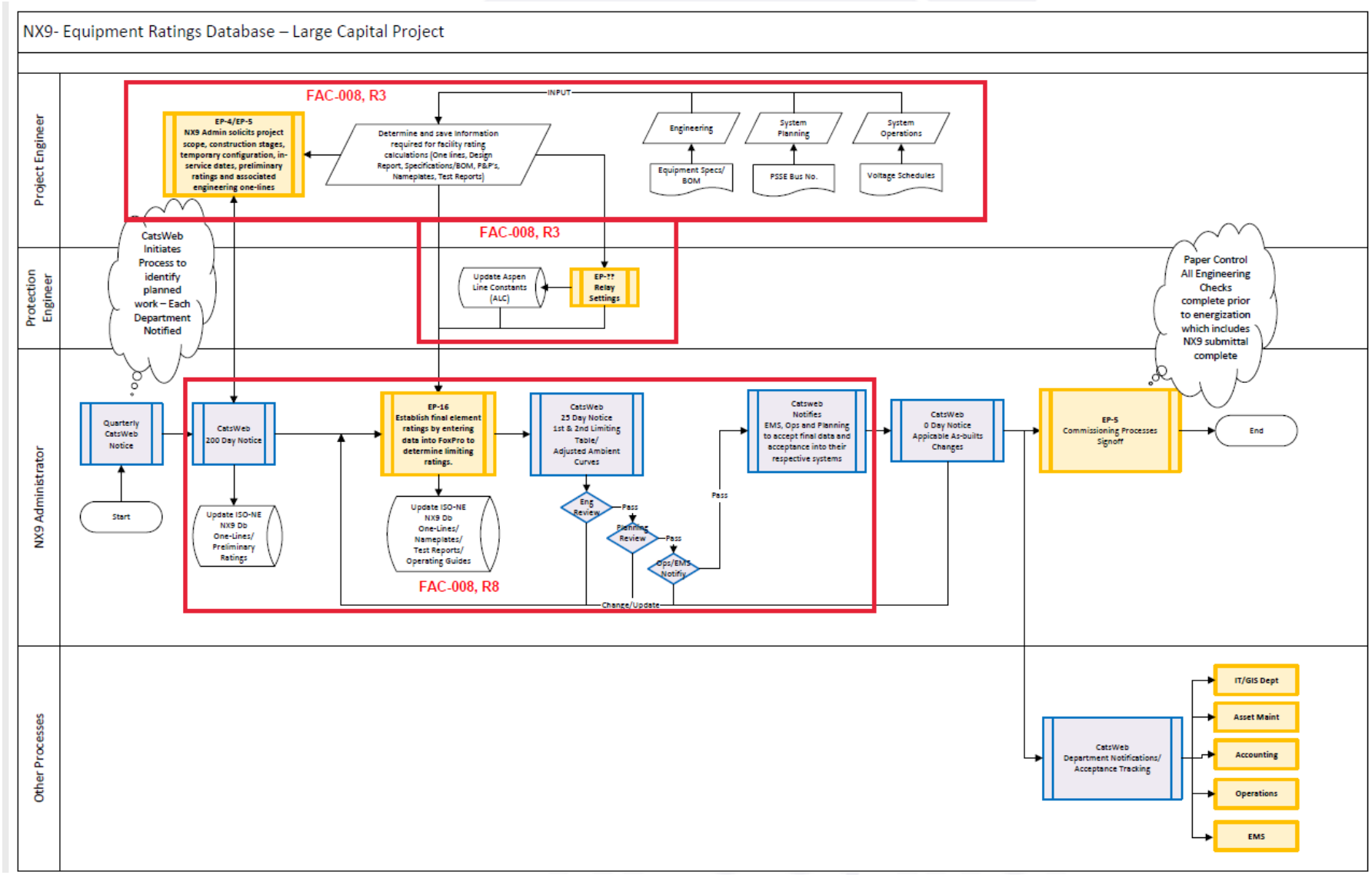
Process Flow Diagram – Existing Process



Process Flow Diagram – Self Audit



Process Flow Diagram – proposed future state



Next Steps

- Schedule a WebEx
- Go over controls questions
- Document answers
- Suggest improvements to existing controls (future state)
  - In this case, may review and discuss Vtransco's proposed controls enhancements
- Capture results in VTransco COP to inform future monitoring

Thank you

My name is Ben Eng

- I can be reached at beng@npcc.org
- Or call/text me at 917-828-4980

- Thank you for your attention!

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

ERO Reliability Metrics: 2020 State of Reliability

An Assessment of 2019 BPS Performance

John Moura, Director of Reliability Assessment and Performance Analysis

NPCC Compliance and Standards Webinar

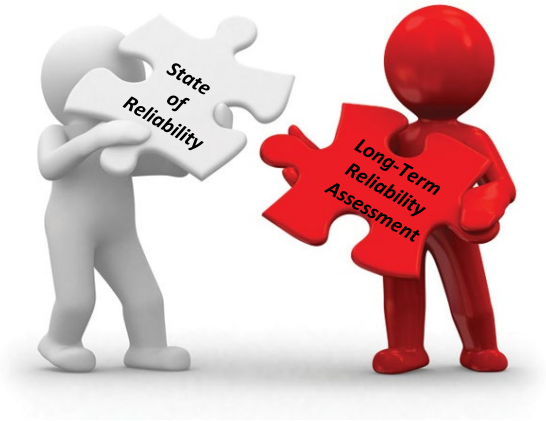
Wednesday, November 18, 2020

RELIABILITY | RESILIENCE | SECURITY




State of Reliability: Objective

- Provide objective and concise information to policymakers, industry leaders, and the NERC Board of Trustees on issues affecting the reliability and resilience of the North American bulk power system (BPS)
  - Identify system performance trends and emerging reliability risks
  - Determine the relative health of the interconnected system
  - Measure the success of mitigation activities deployed



Key Findings

- Improved reliability in 2019
- No category 3, 4, or 5 events
- Frequency response stable or improving
- Conventional generation forced outage rate is down
- Slight uptick in number of Energy Emergencies
- Improved protection system misoperation rate
- No reportable cyber or physical security incidents
- Extreme events caused by winter weather and fire are most severe to BPS
  - Fire-related transmission forced outages in October one of largest simultaneous outage of transmission on record

Report Framework

By the Numbers: North American BPS	Detailed statistics on peak demand, energy, generation capacity, fuel mix, transmission miles, and functional organizations.
Events Analysis Review	Detailed review of qualified events analyzed by the ERO throughout the year. Highlights of published lessons learned are also included.
Reliability Indicators	Set of reliability metrics that evaluate four core aspects of system performance: 1) resource adequacy, 2) transmission performance and availability, 3) generation performance and availability, and 4) system protection and disturbance performance.
Severity Risk Index and Component Analysis	Performance measure of the BPS on a daily basis compared to prior years built from components of generation, transmission and load loss data.
Trends in Priority Reliability Issues	Data and analysis from various NERC data sources are compiled to provide clear insights on a variety of priority reliability issues.

North American BPS:
By the Numbers

4,639,652,736 MWh
2019 Actual Energy

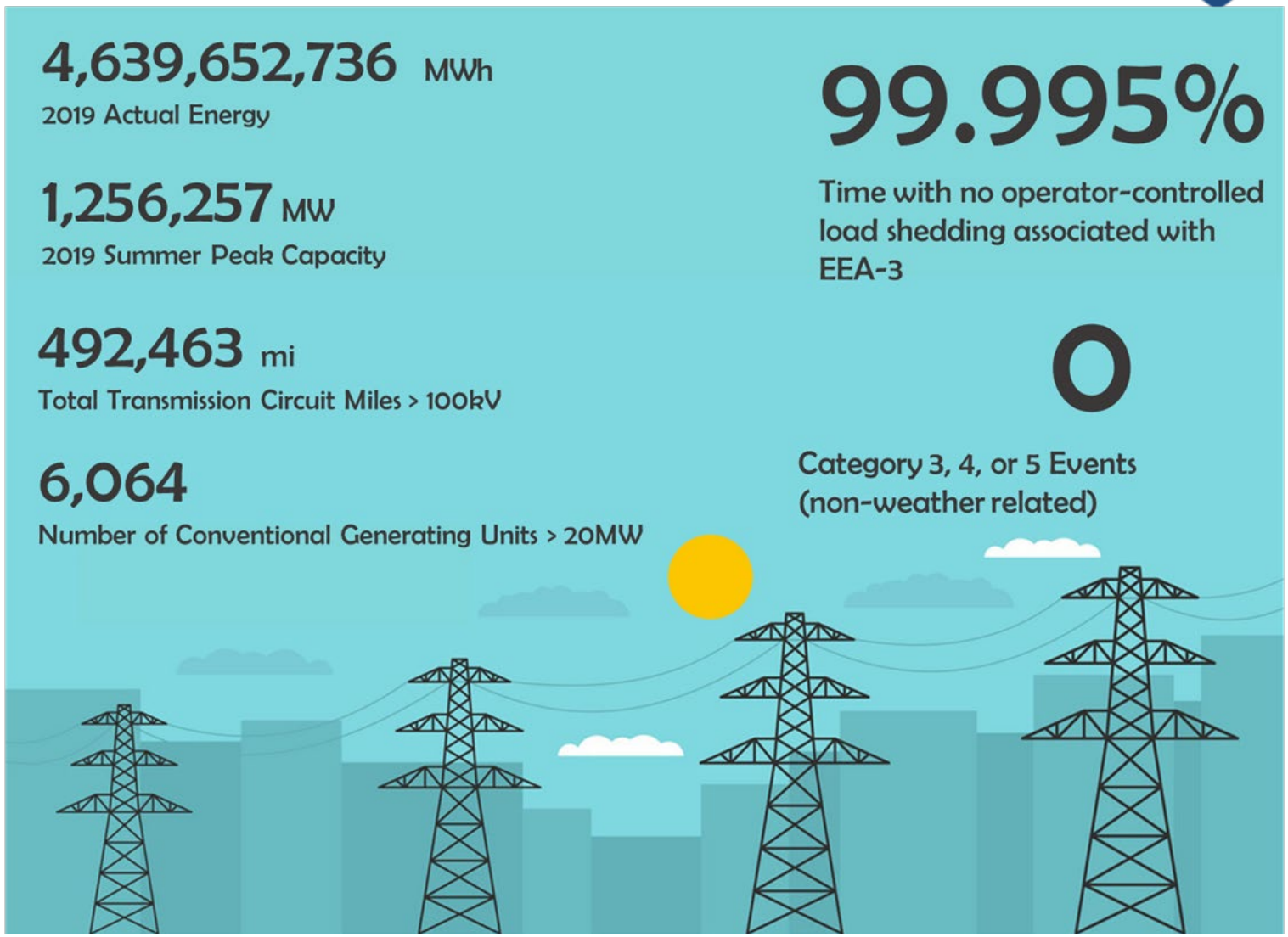
1,256,257 MW
2019 Summer Peak Capacity

492,463 mi
Total Transmission Circuit Miles > 100kV

6,064
Number of Conventional Generating Units > 20MW

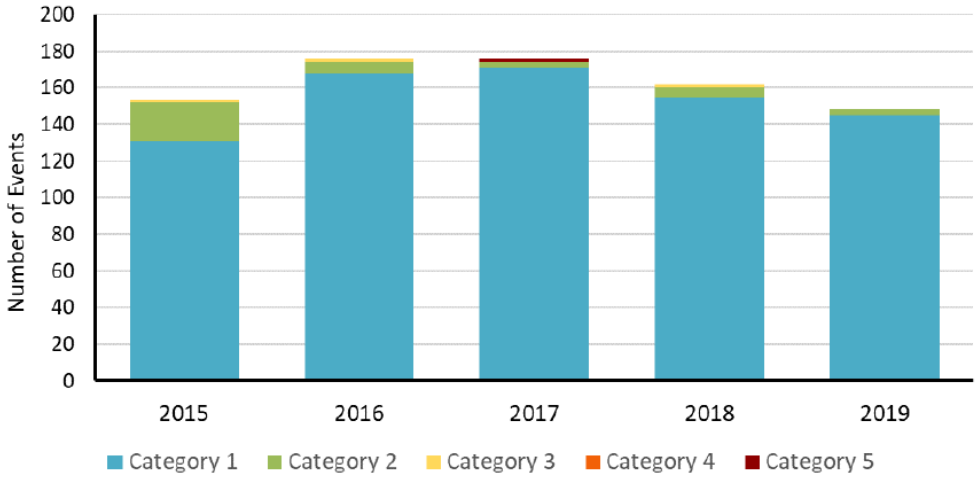
99.995%
Time with no operator-controlled load shedding associated with EEA-3

0
Category 3, 4, or 5 Events (non-weather related)

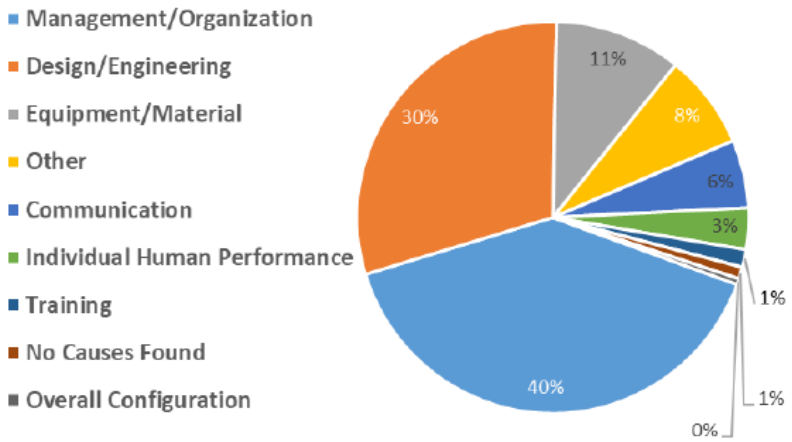


2015 - 2019 Events and Trends

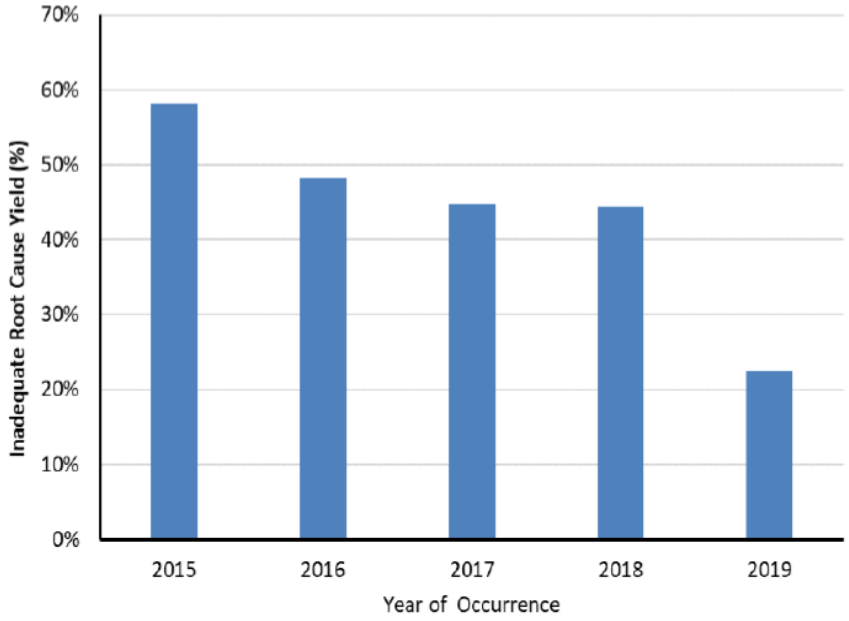
Number of Events per Category by Year



Identified Root Causes



Events with No Root Cause Identified



2015–2019 Identified Root Causes

Reliability Indicator Categories

The reliability indicators represent four core aspects to system performance that are measurable and quantifiable:

- **Resource Adequacy** - Does the system have enough capacity, energy, and ancillary services?
- **Transmission Performance and Availability** - Is the transmission system adequate?
- **Generation Performance and Availability** - What are the energy limitations and outage performance of the generation fleet?
- **System Protection and Distribution Performance** - Can the system remain stable and withstand disturbances?

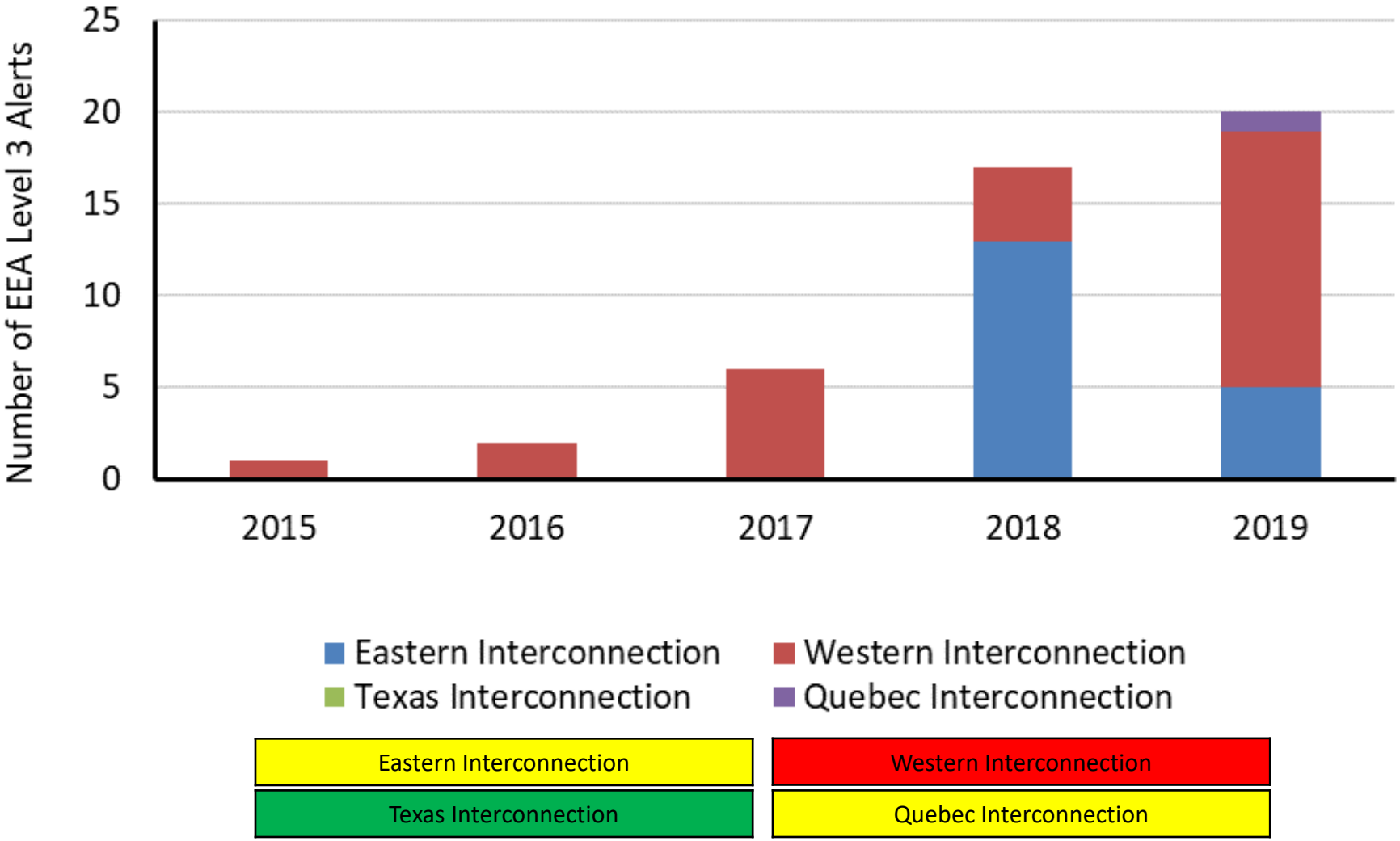
Red – Actionable, key finding

Yellow – Declining, heightened monitoring

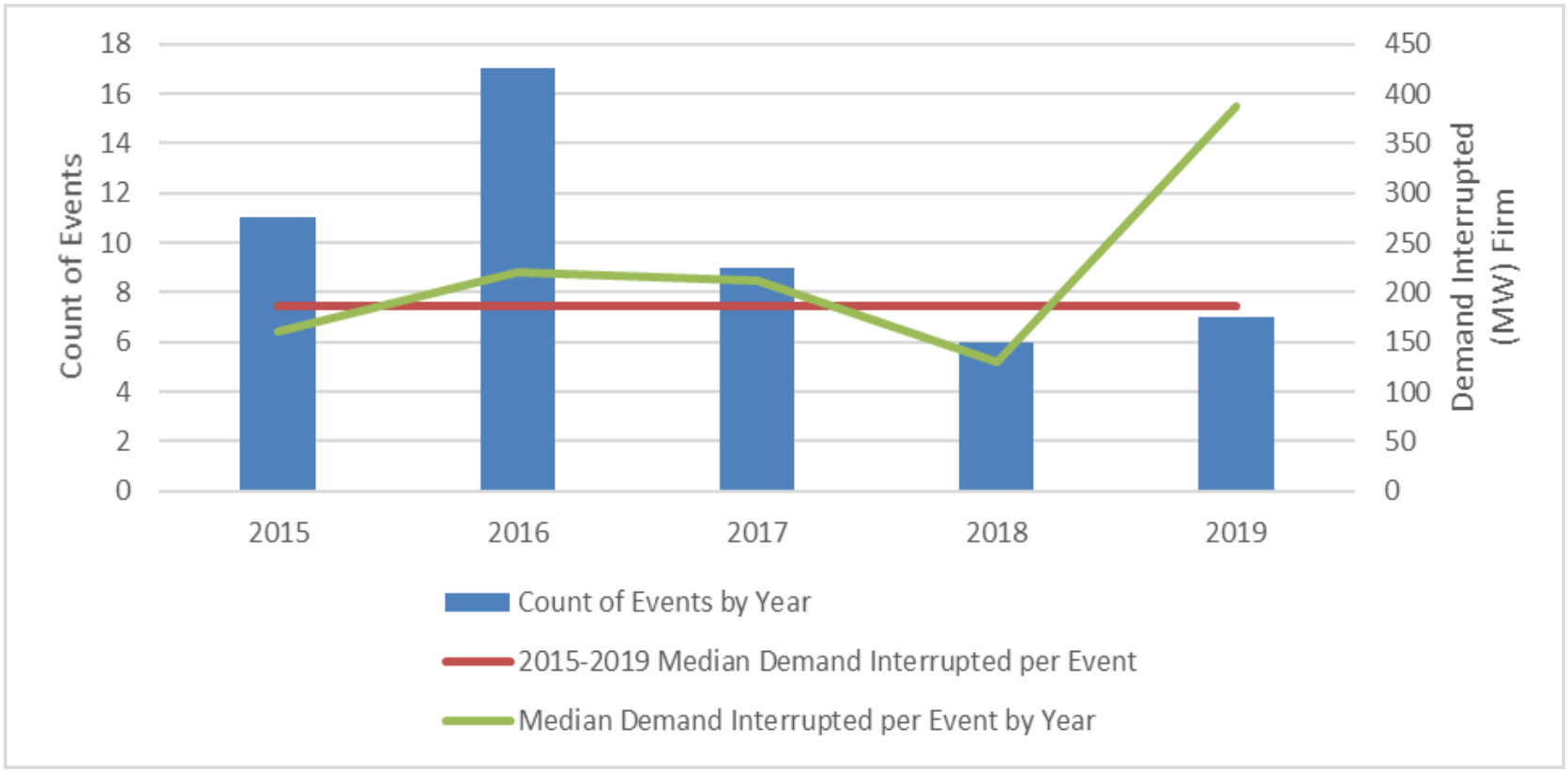
White – Stable or no change

Green – Improving

Reliability Indicators:
Energy Emergencies (Level 3)

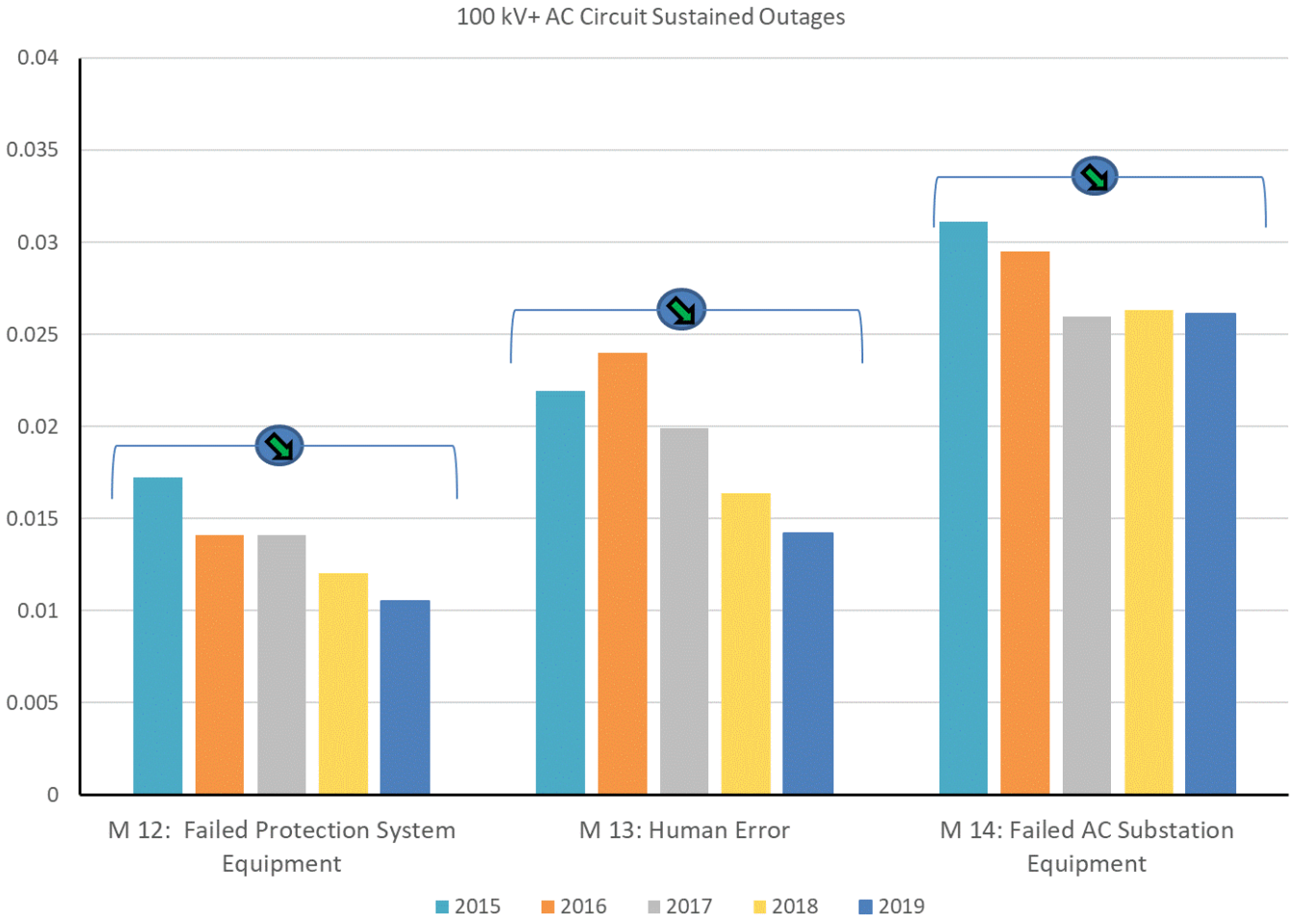


Reliability Indicators:
Loss of Load Transmission-Related Events



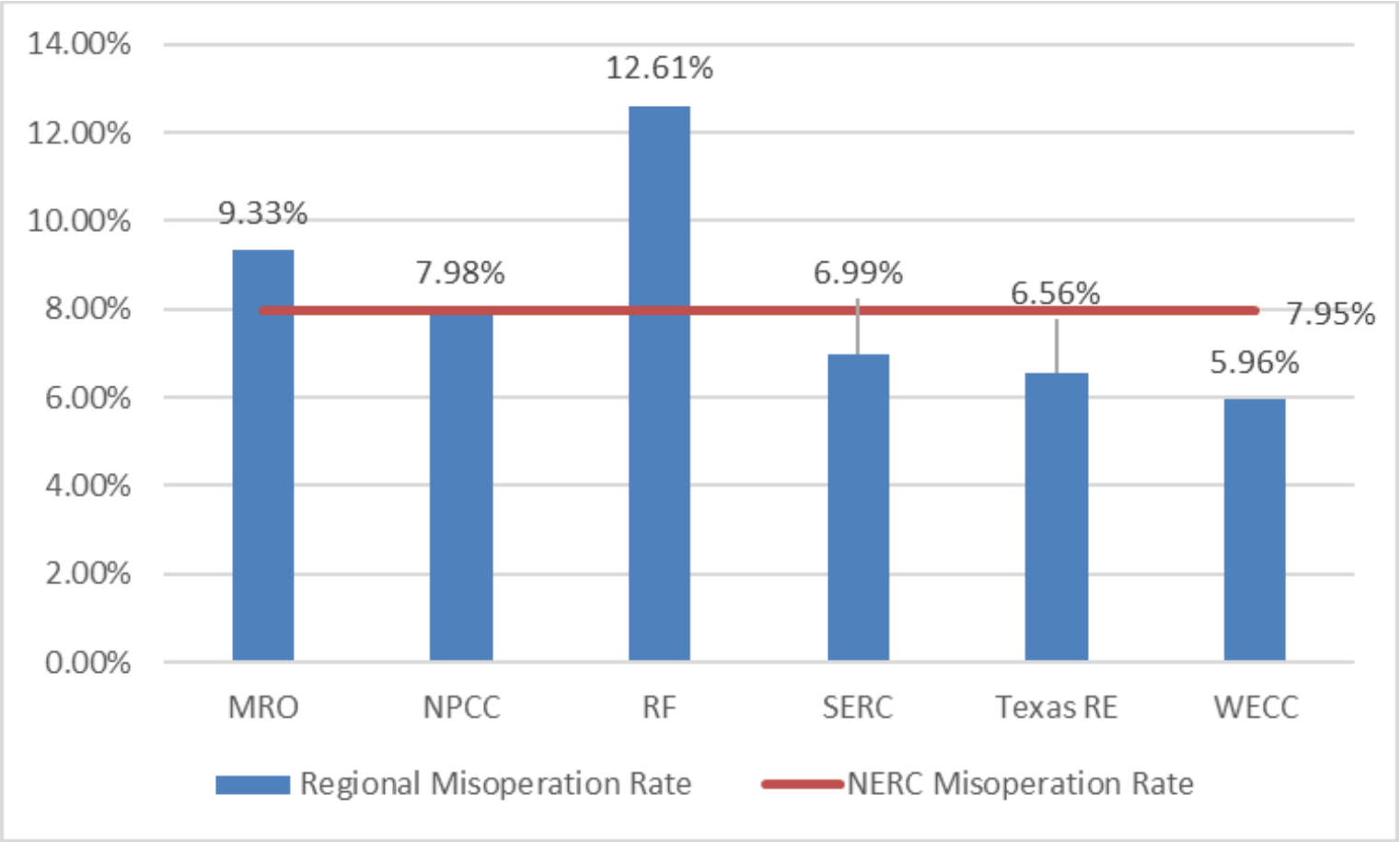
Transmission greater than 100kV

Reliability Indicators: Transmission Outages



Protection System
Human Error
AC Substation Equipment

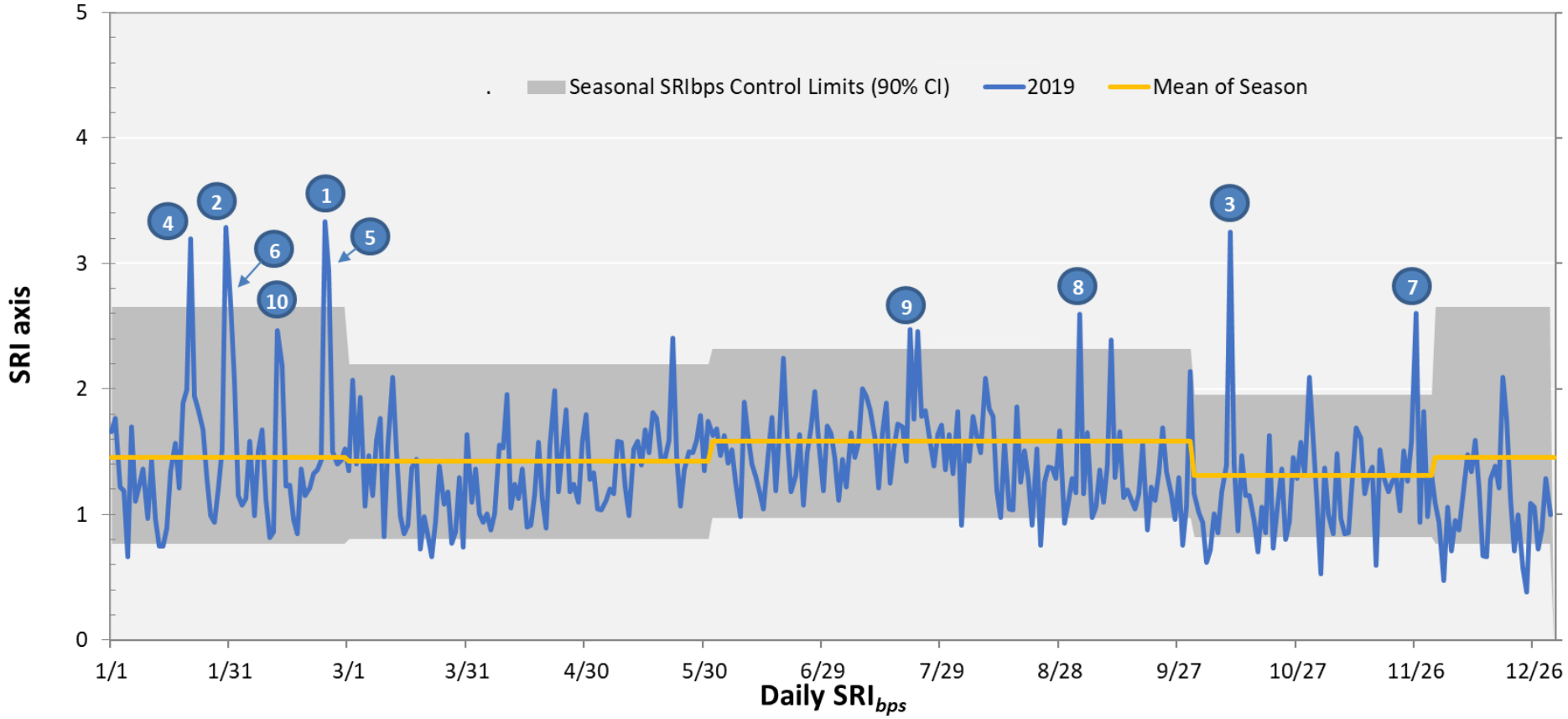
Reliability Indicators:
Protection System Misoperations



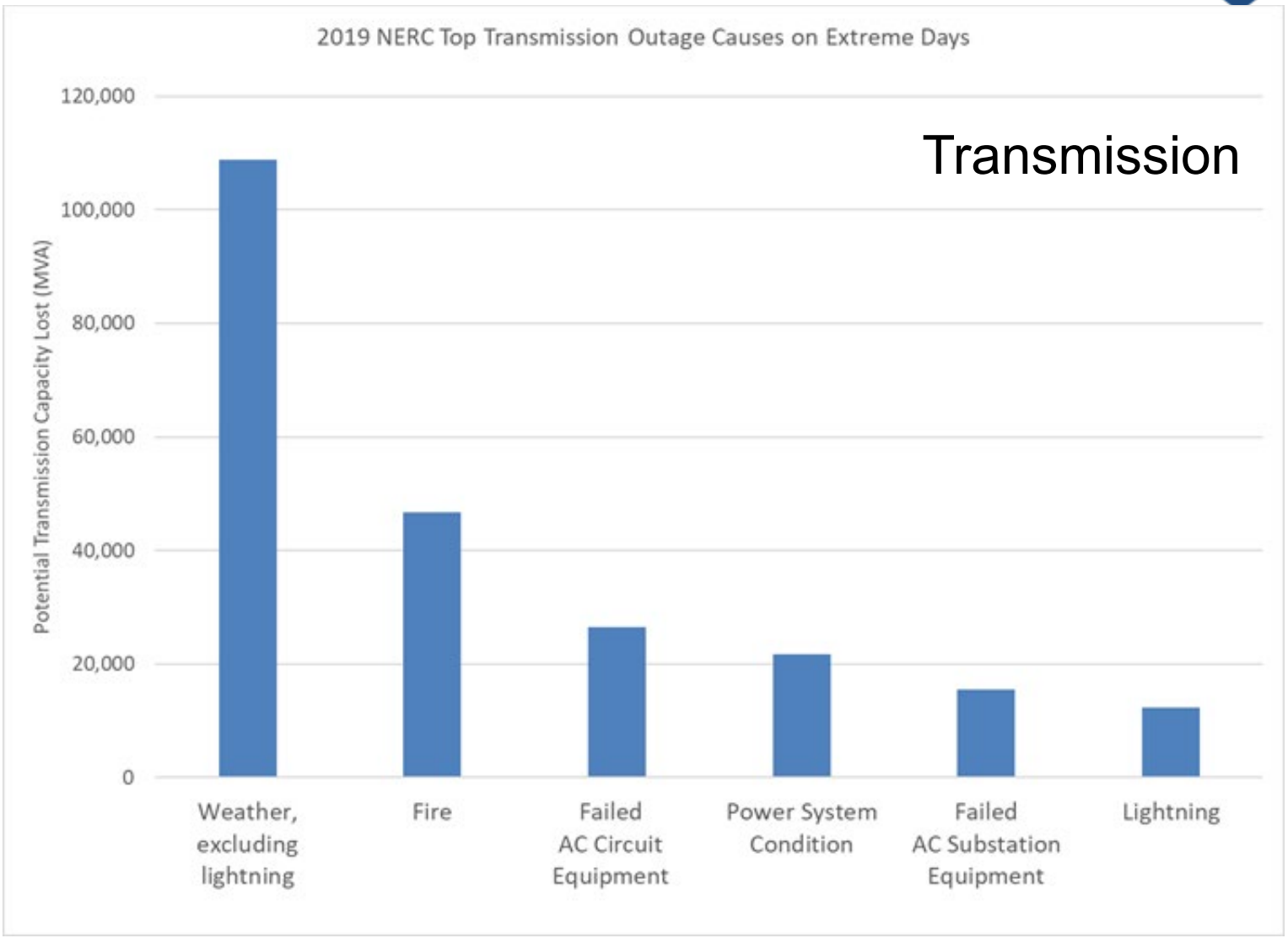
BES Protection Systems

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

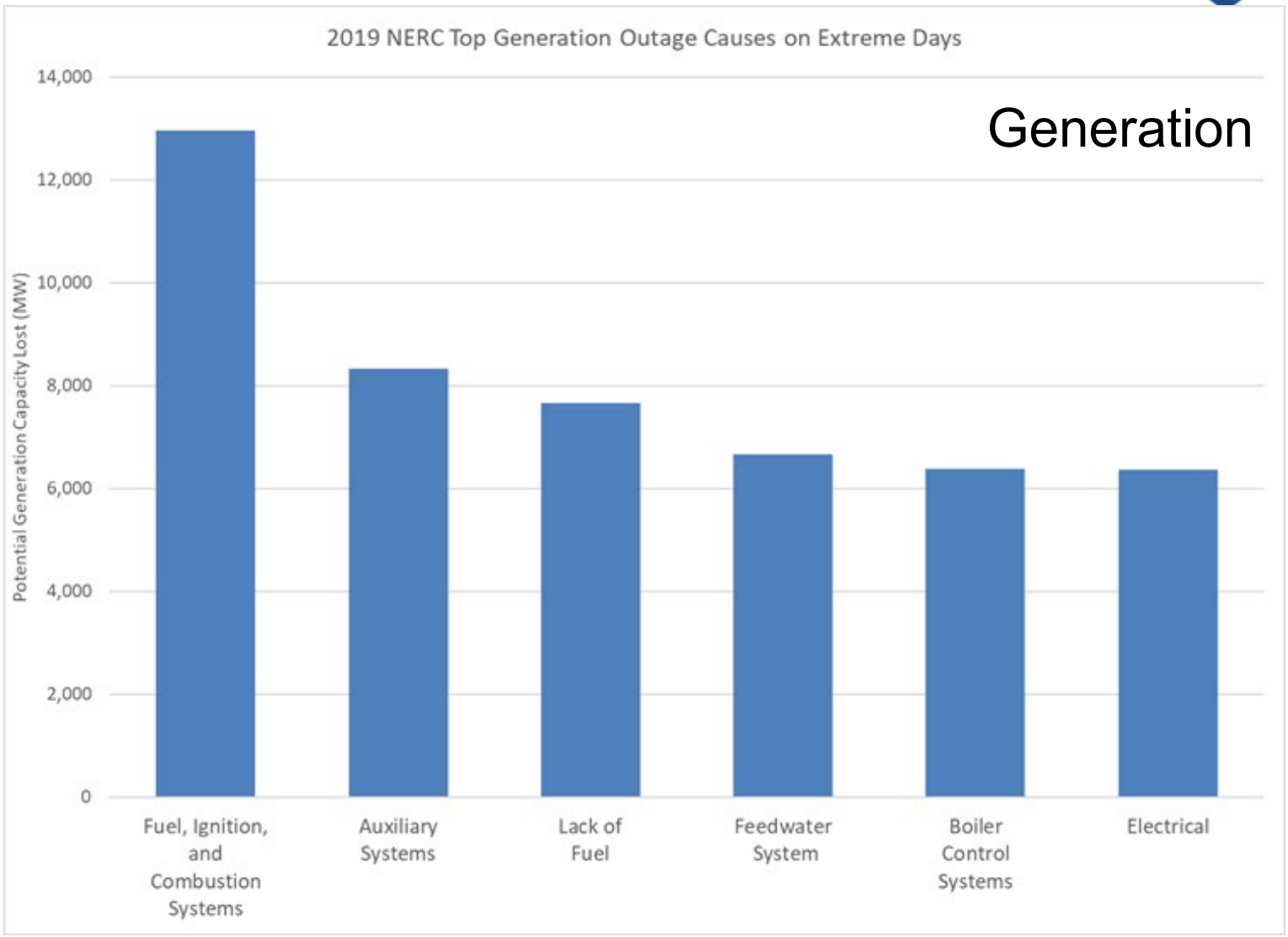
Severity Risk Index:
Top 10 Days in 2019



Priority Reliability Issues Example:
Resilience and Extreme Natural Events



Priority Reliability Issues Example:
Resilience and Extreme Natural Events

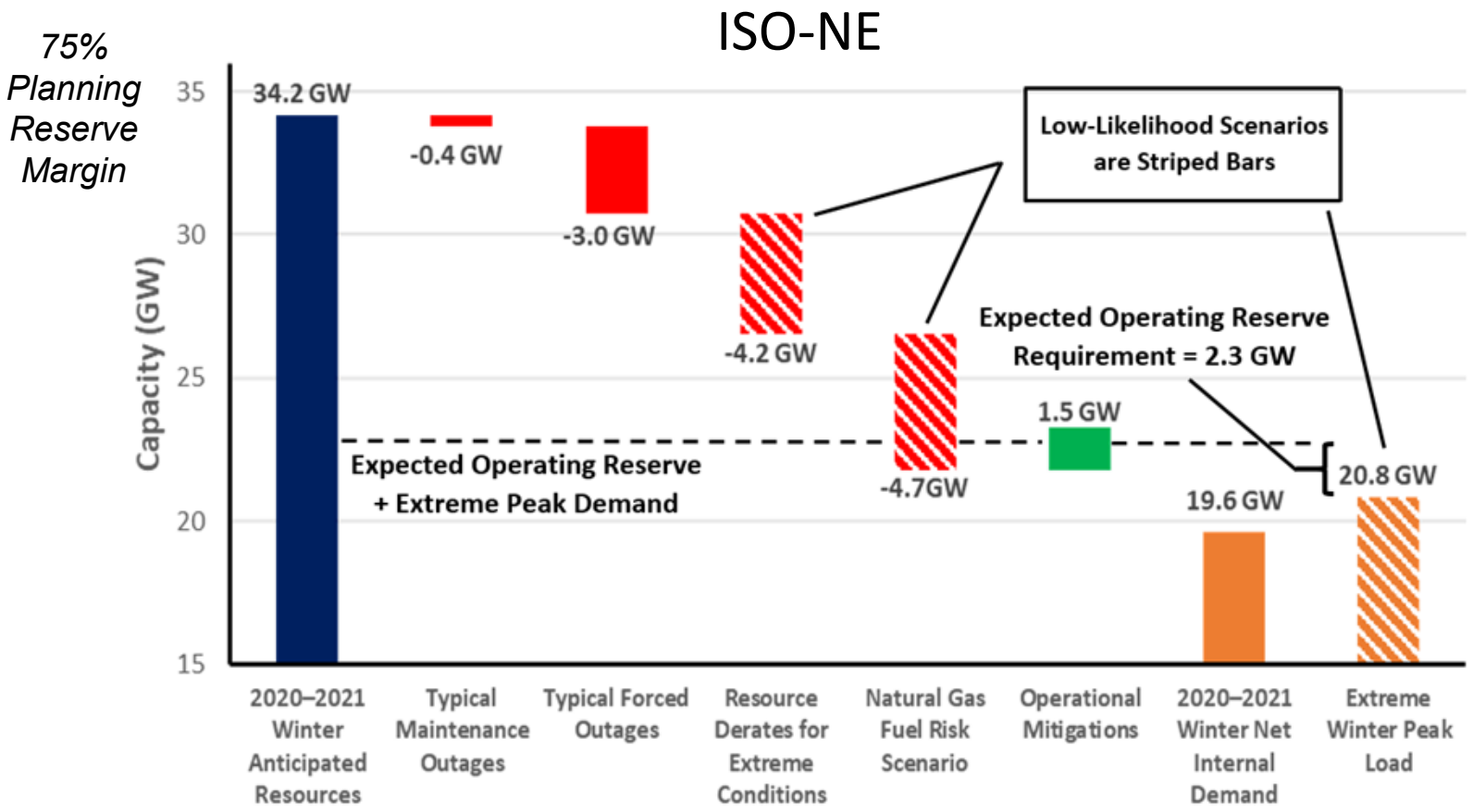


NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

2020/2021 Winter Assessment

2020-2021 Winter: Operational Risk Scenarios

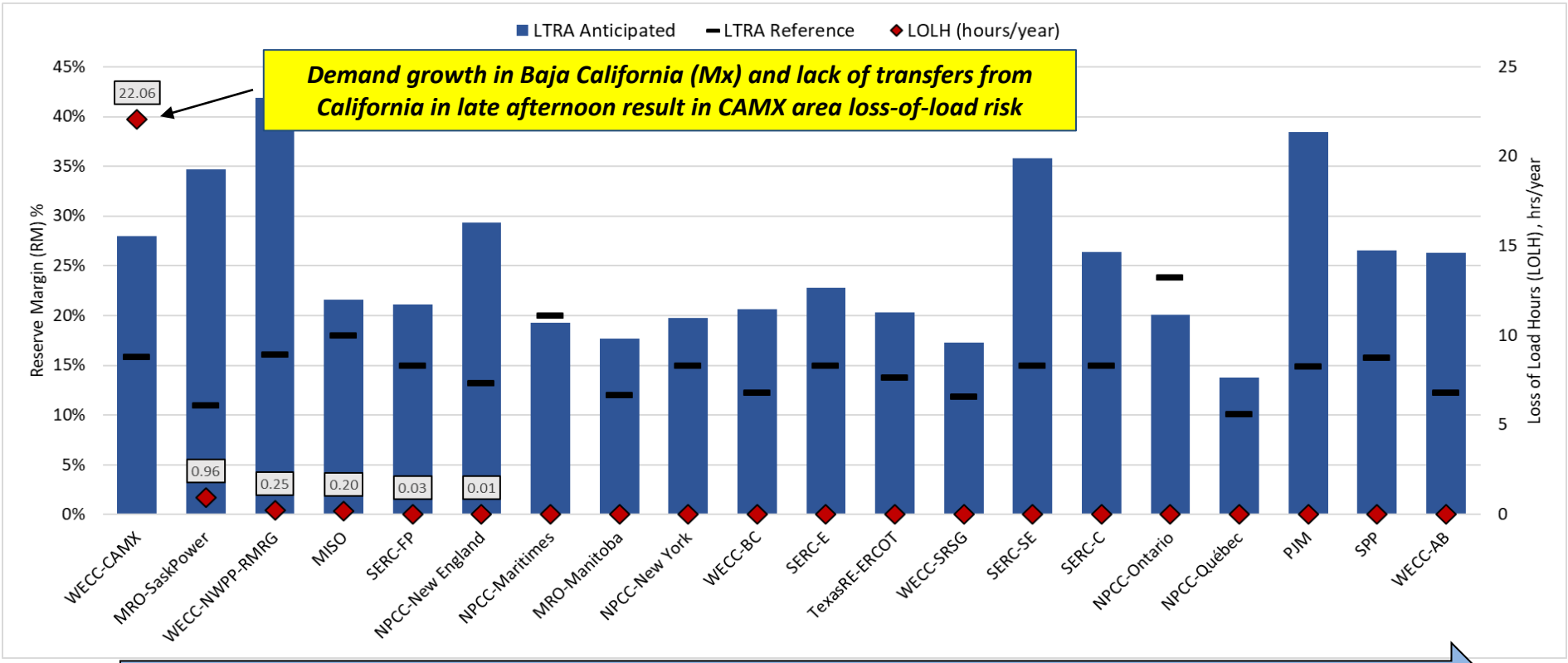
- Operational risk scenarios analyze the effects of extreme conditions on meeting operating reserve targets



2020 LTRA Preview

Finding:
Probabilistic Assessment Highlights Risk Across All Hours

- Probabilistic evaluations of all demand hours identify resource adequacy risks at peak and off-peak
  - Increasing risk is seen in parts of West Interconnection, MISO, and Texas



Reserve Margins and Loss-of-Load Hours (LOLH) for 2022 Peak Season

Important Takeaways

- Performance trends generally positive, though some places appear to be operating closer to the edge.
- Extreme winter weather conditions lead to most significant impacts.
- Emerging fuel mix changes substantially alters the risk profile:
  - Move away from on-site fuel (coal, petroleum and nuclear reductions)
  - Just in time delivery of natural gas backed-up by petroleum
  - Significant growth in distributed energy resources
  - Weather dependencies of wind and solar
- Maintaining cyber and physical security vigilance and hygiene.

Questions and Answers

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

ALIGN

Align Update

NPCC Fall Workshops

November 18, 2020

RELIABILITY | RESILIENCE | SECURITY




Agenda

- Current Events
- Release 1 Functionality and Users
- Evidence Management Guiding Principles
- Update on ERO Secure Evidence Locker
- Release 1 Training
- Access Provisioning
- FAQs

Current Events

- Facilitated registered entity testing exercise of Release 1 functionalities
- Finalizing training materials (i.e., videos, user guide, etc.)
- ERO SEL under construction – First demo was last week
- Regional adoption workshops for ERO Enterprise staff in progress

Align Release 1: What to expect as a registered entity?

Stakeholder Group

Registered Entities

Release 1 Functionality

- Create and submit Self-Reports and Self-Logs
- Create and manage mitigating activities (informal) and Mitigation Plans (formal)
- View and track open Enforcement Actions (EAs) resulting from all monitoring methods
- Receive and respond to Requests for Information (RFIs)
- Receive notifications and view dashboards on new/open action items
- Generate report of standards and requirements applicable to your entity
- Manage user access for your specific entity
- Manage evidence supporting R1 functionality securely via separate Evidence Locker(s)

Align Future Releases: What to expect?

Release 2 Functionality Q2 2021

- Technical Feasibility Exceptions (TFEs)
- Periodic Data Submittals
- Self-Certifications
- Additional enhancements identified from R1 as needed
- CFRs, JROs and Attestation in Align
- Expand use of Evidence Lockers to include evidence submitted for these activities

Note: The monitoring methods above will be managed in existing systems during the gap between R1 and R2

Release 3 Functionality Q4 2021

- Compliance Planning (i.e., Risk, CMEP Implementation Plan, Inherent Risk Assessment, Internal Controls Evaluation, Compliance Oversight Plan)
- Compliance Audit
- Spot Check
- Compliance Investigations
- Complaints
- Expand use of evidence lockers to include evidence submitted for these activities

Evidence Management Guiding Principles

- All registered entity-provided evidence, unless prohibited by a standard, will go into the SEL
  - All registered entity lockers must meet ERO SEL functional requirements
- ERO Enterprise workflow and work products will be in the ERO Enterprise Align tool.
- The ERO Enterprise will enhance work products (e.g., working papers) to support conclusions without the need to store data for extended periods, minimizing data protection risk.

NOTE: The Align team will achieve this through training, guidance, oversight activities, and other outreach.

Evidence Lockers: What are they?

- Highly secure, isolated, on-premises environments
  - Collect and protect evidence
  - Enable submission by authorized and authenticated entity users
  - Provide compartmentalized analysis of evidence in temporary, isolated, disposable environments
  - Does not interface with any other systems
- Evidence in these environments is:
  - Encrypted immediately upon submission
  - Securely isolated per entity
  - Never extracted
  - Never backed up
  - Subject to proactive and disciplined destruction policy

Release 1 Training: What is the approach?

- Train-the-Trainer approach
- The NERC Training Department is producing all materials.
  - NERC training website hosts training videos and user guide.
  - Dedicated training environment for Regions and registered entities.
- Training leads have been identified for each Region.
  - The training leads will train the Regions and registered entities.
  - Trainings will be 100% remote due to COVID-19.

Release 1 Training: What will it include?

- Align Release 1 functionality
- Evidence Locker capability to support Release 1 activities
- Regional changes in business processes for Release 1 activities
- Management of CMEP activities to include current legacy systems (Start/Stop/Continue)

Access Provisioning Overview

- All Align users must have an **active ERO Portal account** prior to accessing Align (https://eroportal.nerc.net/)
- PCCs will manage access for their organizations within the ERO Portal
- Prior to go-live, NERC will ensure all PCCs with ERO Portal Accounts are set up as an **Align Registered Entity Submitter** and the **Entity Administrators** responsible for approving access requests
- Same log-ins for production and the training environment

FAQs

- There are answers to more than 120 questions posted on the Align Project FAQ page, which can be sorted using the Search feature
- Submit questions to askalign@nerc.net

- NPCC Change Agents:
  - Kimberly Griffith, kgriffith@npcc.org
  - Jason Wang, jwang@npcc.org

- Align Readiness Pulse Check Survey

Questions and Answers

2021 ERO Compliance Monitoring and Enforcement Program (CMEP) Implementation Plan (IP)

Jacqueline Jimenez

Manager, Compliance

Implementation Plan Background

Purpose of the CMEP IP

- Annual CMEP-related operating plan for NERC and Regional Entities
- Implementation of risk-based approach for CMEP activities

Timeline

- NERC final IP with links to regional schedules is typically posted in November
- Updates may occur throughout year

CMEP IP Development

Risk Elements

Data-driven and expert judgement of ERO Enterprise staff	Use of ERO Enterprise publications	Identify and to prioritize interconnection and continent-wide, as well as regional, risks to the reliability of the bulk power system	Not intended to be a representation of just “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

2021 CMEP IP Highlights

Used the enhanced, easier-to-use format introduced in the 2020 CMEP IP

- 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

COVID-19

- Summary of industry guidance
- Prioritize monitoring activities and risks that benefit the most from on-site components when conditions allow
- Risks reflected in Risk Element write-ups
- ERO Enterprise may consider reviewing requirements related to personnel training

2021 Risk Elements Comparison

Table 1: Comparison of 2020 Risk Elements and 2021 Risk Elements	
2020 Risk Elements	**2021 Risk Elements**
Management of Access and Access Controls	Remote Connectivity and Supply Chain
Insufficient Long-Term and Operations Planning Due to Inadequate Models	Poor Quality Models Impacting Planning and Operations
Loss of Major Transmission Equipment with Extended Lead Times	Loss of Major Transmission Equipment with Extended Lead Times
Inadequate Real-time Analysis During Tool and Data Outages	Inadequate Real-time Analysis During Tool and Data Outages
Improper Determination of Misoperations	Determination and Prevention of Misoperations
Gaps in Program Execution	Gaps in Program Execution
Texas RE: Resource Adequacy	

Areas of Focus

Table 2: Remote Connectivity and Supply Chain			
Standard	**Requirement**	**Entities for Attention**	**Asset Types**
CIP-005-6	R2	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner	Back up Control Centers Control Centers Data Centers Generation Facilities Substations
CIP-007-6	R1	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner	Backup Control Centers Control Centers Data Centers Generation Facilities Substations
CIP-010-3	R1	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner	Backup Control Centers Control Centers Data Centers Generation Facilities Substations
CIP-013-1	R1, R2	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner	

Areas of Focus

Table 3: Poor Quality Models Impacting Planning and Operations			
Standard	**Requirements**	**Entities for Attention**	**Rationale**
MOD-026-1	R2	Generator Owner Transmission Planner	Ensure adequate models of generation
MOD-027-1	R2	Generator Owner Transmission Planner	Ensure adequate models of generation
MOD-033-1	R1, R2	Planning Coordinator Reliability Coordinator Transmission Operator	Ensure accurate System models.

Areas of Focus

Table 4: Loss of Major Transmission Equipment with Extended Lead Times			
Standard	**Requirements**	**Entities for Attention**	**Rationale**
TPL-001-4	R2.1.5	Planning Coordinator Transmission Planner	Ensure that unavailability of major Transmission equipment has been considered in the entity's spare equipment strategy.

Areas of Focus

Table 5: Inadequate Real-time Analysis during Tool and Data Outages			
Standard	**Requirements**	**Entities for Attention**	**Rationale**
IRO-008-2	R4	Reliability Coordinator	Ensuring situational awareness is maintained regardless of advanced applications which affect RTA status
TOP-001-4	R13	Transmission Operator	Ensuring situational awareness is maintained regardless of advanced applications which affect RTA status

Areas of Focus

Table 6: Determination and Prevention of Misoperations			
Standard	**Requirements**	**Entities for Attention**	**Rationale**
PRC-004-5(i)*	R1, R5	Generator Owner Transmission Owner	Ensure proper analysis of protection system operations.
PRC-027-1	R1, R3	Generator Owner Transmission Owner	Ensure proper analysis of lessons learned from misoperations.

Areas of Focus

Table 7: Gaps in Program Execution			
Standard	**Requirements**	**Entities for Attention**	**Rationale**
CIP-010-3	R1	Balancing Authority Generator Owner Transmission Operator Transmission Owner Reliability Coordinator	Ensuring entities maintain complex programs which handle large amounts of data, e.g., accurate inventories of equipment, following asset transfers, addition of new equipment, etc.
FAC-003-4	R1, R2, R3, R6, R7	Generator Owner Transmission Owner	
FAC-008-3	R6	Generator Owner Transmission Owner	
PRC-005-6	R3	Generator Owner Transmission Owner	

Resources

- 2021 ERO Enterprise CMEP IP

https://www.nerc.com/pa/comp/CAOneStopShop/ERO%20CMEP%20Implementation%20Plan%20-%202021.pdf

Questions?

jjimenez@npcc.org

Supply Chain Risk Management

Jenifer Farrell

Jason Wang

Supply Chain Risk Management

- CIP-005-6 – Cyber Security – Electronic Security Perimeter(s), by three months (October 1, 2020);
- CIP-010-3 – Cyber Security – Configuration Change Management and Vulnerability Assessments, by three months (October 1, 2020);
- CIP-013-1 – Cyber Security – Supply Chain Risk Management, by three months (October 1, 2020);

Frequently Asked Questions

Supply Chain – Small Group Advisory Session (SGAS)

- 2018 FAQ
- 2019 FAQ

Implementation Guidance and Guidelines

North American Transmission Forum (NATF)

- Cyber Security Supply Chain Risk Management Guidance
- ERO Endorsed Guidance

Edison Electric Institute (EEI)

- Procurement Contract Language

NERC Resources

- Cyber Security Supply Chain Risk Management Plan
- CIP-013 RSAW

Implementation Guidance and Guidelines

Critical Infrastructure Protection Committee (CIPC)

- Risk Management – An overview of topics such as identifying, assessing, and mitigating threats and procurements, installations and updating the risk management plan.
- Secure Equipment Delivery – Highlights some of the aspects to consider regarding secure transportation and delivery of systems and components, from component manufacturers to integrators, to vendors, and ultimately to the Bulk Electric System (BES).
- Risk Considerations for Open Source Software – An overview defining open source software and risks to consider if your entity has open source software
- Best Practices for Small Entities – Although CIP-013-1 is not applicable to low-impact BES Cyber Systems, this white paper identifies a catalog of supply chain risk management practices for consideration by small registered entities with low-impact BES Cyber Systems.

NERC Resource Pages

- Supply Chain Working Group (SCWG)
  - Webinars, Guidelines, Presentations
- Supply Chain Risk Mitigation Program
  - Background Documents, Compliance Information, Discussions and Recommendations, Data Requests, Endorsed Implementation Guides

NPCC Resources

- Compliance Bulletin
  - CIP-013 – Supply Chain Risk Management Resources
  - Recommend Practices
  - FAQ

FERC Order No. 850

- RM17-13-000
  - Electronic Access Control or Monitoring Systems (EACMS)
  - Physical Access Control Systems (PACS)
  - Low impact BES Cyber Systems
  - Protected Cyber Assets

Future Plans for CIP-013-2

FERC Order 850 (October 18, 2018)

- FERC directs NERC modify CIP-013 to include EACMS associated with medium and high impact BES Cyber Systems.
- FERC accepted NERC's commitment to evaluate the risks of PACSs and PCAs (in addition to low impact BES Cyber Systems)

NERC Cyber Security Supply Chain Risks Report (May 17, 2019)

- NERC recommends CIP-013 to address Physical Access Control Systems (PACSs) to high and medium-impact BES Cyber Systems.
- NERC recommends additional studies for low-impact BES Cyber Systems and PCAs.
- NERC recommends CIPC Supply Chain Working Group develop a guideline to assist entities in applying supply chain risk management plans to low impact BES Cyber Systems and PCAs.

Standards drafting team (September 2019)

- Creation of CIP-013-2 to include EACMS and PACS.
- Final ballot approval estimated November 2020

2020 Current Events and Predicted Future

- Send to BOT for Approval
- Send to FERC for Filing
- FERC approval estimated 2021
- Estimated Effective date in 2022

Questions

Jenifer Farrell

jvallace@npcc.org

FERC NOI ERO Response Highlights

NPCC Fall 2020

Topics in this Presentation

1. ERO FERC NOI Response Timeframe
2. Questions being answered
3. ERO Response Highlights

The ERO comments are undergoing management review and are subject to change based on that review.

FERC NOI Response Timeframe

FERC NOI: Equipment and Services Produced or Provided by Certain Entities Identified as Risks to National Security (September 17, 2020), Docket No. RM20-19-000

NERC plan to file Response by file November 23, 2020

- As of this presentation comments are still in draft and undergoing management review.

Questions to be Answered

FERC NOI seeks comment on the following:

(1)The extent of the use of telecommunications equipment and services provided by certain foreign entities identified as risks to national security related to BES operations;

(2)The risks to BES reliability and security posed by the use of equipment and services provided by the identified entities;

(3)Whether the CIP Reliability Standards requirements adequately mitigate the identified risks;

(4)Strategies that entities have implemented or plan to implement – in addition to compliance with the mandatory CIP Reliability Standards – to mitigate the risks associated with use of equipment and services provided by the identified entities; and

(5)Other methods the Commission may employ to address this matter, including working collaboratively with industry to raise awareness about the identified risks and assisting with mitigating actions

Question Response Q1

A. ERO Enterprise recognizes the importance of managing supply chain risks and supports entities in identifying equipment and services that present heightened risks to the BPS as a result of their supply chain.

NERC level 2 Alerts Issued:

1. OCT. 2017: Alert regarding supply chain risk (Kaspersky anti-virus software)
2. July 2019: Alert regarding supply chain risks related to certain Chinese manufacturers of telecommunication equipment.
3. July 2020: Alert requiring registered entities to report on equipment used that is banned by an Executive Order issued concerning security of the BPS (NERC/FERC White Paper)

Question Response Q2 and Q3

B. NERC Reliability Standards help to address the risk posed by potential compromise of telecommunications equipment and services.

- Focused on new and existing standard to mitigate a supply chain risk broadly.
- Some of these standards and requirements are only just being developed or implemented:
  - Oct 1, 2021 (CIP-013-1)
  - July 1, 2022 (CIP-012-1)
- Analyst and effectiveness review of controls:
  - Supply chain effectiveness review
  - Study of electronic access controls for assets containing low impact BES Cyber Systems (July 1, 2021).

Standards to Mitigate Risk Q2 and Q3:

Compromised Telecommunications Equipment:

- CIP-013-1 (Effective Oct. 1, 2020)
- CIP-005-6, Req. R2, Parts 2.4 and 2.5:
- CIP-010-3, Req. R1, Part 1.6
- Low impact BES Cyber Systems

Compromised or Misuse of Existing Equipment and Services:

- CIP-002-5.1a
- CIP-005-6
- CIP-007-6
- CIP-008-6
- CIP-009-6
- CIP-012-1

  (Effective July 1, 2022)

Risk Mitigation should Telecommunications Equipment become Compromised:

- IRO-002-5
- TOP-001-4
- COM-001-3
- EOP-008-2

Question Response Q4 and Q5

C. The ERO Enterprise supports activities beyond mandatory Reliability Standards to help industry mitigate risk should equipment or services be compromised.

NERC Board Adopted as Resolutions:

1. Engage in a cyber security supply chain risk study (Electric Power Research Institute)
2. Communicates supply chain risks to industry;
3. Develop of white papers addressing for supply chain management best practices
4. Evaluates the effectiveness of supply chain standards.

E-ISAC

1. Information Sharing (Threats, Vulnerabilities, Mitigation, Awareness)
2. Coordination with: DOE, PNNL, CRISP
3. GridEx

Industry Trade Groups: Example: NATF, NAGF

NERC Reliability and Security Technical Committee ("RSTC")

ERO Outreach Activities

telecommunications
telecommunications

Conclusion

- The ERO Enterprise supports Responsible Entities in assessing telecommunication equipment and services to identify risks posed
- The ERO Enterprise continues to work with industry, through standards development projects and other activities, to help ensure the risks described above are addressed and mitigated if needed.

  - As of this presentation comments are still in draft and undergoing management review.


Questions?

FERC CIP Lessons Learned

Published October 2, 2020

https://www.ferc.gov/news-events/news/ferc-staff-report-details-lessons-learned-cip-reliability-audits

Michael Stuetzle
Cecil Elie

Overview

- The report documents the lessons learned from FERC-led CIP audits conducted during the 2020 Fiscal Year (October 1, 2019 to September 30, 2020)
- It is an anonymized, public report to benefit NERC, the Regional Entities, and registered entities
- It includes mapping to relevant NIST documentation
- The end of the report also includes a summary of the lessons learned from each of the past 3 fiscal years

Standards in Scope

1. CIP-002-5.1a – BES Cyber System Categorization
2. CIP-003-8 – Security Management Controls
3. CIP-004-6 – Personnel & Training
4. CIP-005-5 – Electronic Security Perimeter(s)
5. CIP-006-6 – Physical Security of BES Cyber Systems
6. CIP-007-6 – Systems Security Management
7. CIP-008-5 – Incident Reporting and Response Planning
8. CIP-009-6 – Recovery Plans for BES Cyber Systems
9. CIP-010-2 – Configuration Change Management and Vulnerability Assessments
10. CIP-011-2 – Information Protection

High Level Summary

1. Ensure that all BES Cyber Assets are properly identified.
2. Ensure that all substation BES Cyber Systems are properly categorized as high, medium, or low impact.
3. Ensure that electronic access to BES Cyber System Information (BCSI) is properly authorized and revoked.
4. Consider having a dedicated visitor log at each Physical Security Perimeter (PSP) access point.
5. Consider locking BES Cyber Systems' server racks where possible.
6. Inspect all Physical Security Perimeters (PSPs) periodically to ensure that no unidentified physical access points exist.
7. Review security patch management processes periodically and ensure that they are implemented properly.
8. Consider consolidating and centralizing password change procedures and documentation.
9. Ensure that backup and recovery procedures are updated in a timely manner.
10. Ensure that all remediation plans and steps taken to mitigate vulnerabilities are documented.
11. Ensure that all procedures for tracking the reuse and disposal of substation assets are reviewed and updated regularly.
12. Consider evaluating the security controls implemented by third parties regularly and implement additional controls where needed when using a third party to manage BES Cyber System Information (BCSI).

1. Ensure that all BES Cyber Assets are properly identified.

- CIP-002-5.1a R1
- In some cases entities did not identify BES Cyber Assets equipment performing supporting functions.
- For example, several entities misidentified Cyber Assets as communications equipment instead of BES Cyber Assets.
- The FERC report links to a NERC document which can be a helpful resource.

2. Ensure that all substation BES Cyber Systems are properly categorized as high, medium, or low impact.

- CIP-002-5.1a R1 Attachment 1 Criterion 2.5
- In some cases entities did not properly consider the interdependency of relay schematics and configurations between control houses containing separate voltage levels.
- For example, 138 kV breaker failure relays can trip 345 kV buses, and as a result can impact 345 kV BES Cyber Systems classified as medium impact.

3. Ensure that electronic access to BCSI is properly authorized and revoked.

- CIP-004-6 Requirements R4 & R5
- Some entities did not consistently apply their documented process(es) to properly authorize, or in cases of termination, revoke, employees' access to BCSI.
- In some instances access was granted to electronic BCSI storage locations in a manner that differed from the entity's documented program and in other instances entities did not deactivate user network accounts in a timely manner.

4. Consider having a dedicated visitor log at each Physical Security Perimeter (PSP) access point.

- CIP-006-6 Requirement R1
- Certain entities share a single visitor log between multiple access points within a single PSP, which necessitates moving the log back and forth between access points.
- Could lead to loss of control of the logs and decrease the security posture of the PSP
- NPCC has observed issues arise where not all of the required fields of the visitor log were completed.

5. Consider locking BES Cyber Systems' server racks where possible.

- CIP-006-6 Requirement R1
- Entities' server racks located in their control centers and substations typically have the capability to be locked. Yet, not all entities consistently use this capability.
- This can potentially tie in with CIP-007 R1.2 for protecting against the use of unnecessary physical input/output ports.

6. Inspect all PSPs periodically to ensure that no unidentified physical access points exist.

- CIP-006-6 Requirement R1
- Some entities did not consider access points, often in the ceilings or other locations, that are large enough for a person to gain access to the PSP, such as maintenance access points.

7. Review security patch management processes periodically and ensure that they are implemented properly.

- CIP-007-6, Requirement R2
- FERC observed areas for improvement in
  - Understanding the proper scope of security patch applicability,
  - Procedures for tracking applicable security patches, and
  - Controls to ensure all applicable security patches are installed or a mitigation plan is in place.
- NPCC has also observed “silos” among business units which led to issues in evaluating, tracking, and applying all relevant security patches

8. Consider consolidating and centralizing password change procedures and documentation.

- CIP-007-6, Requirement R5
- Entities that did not use a centralized password database encountered difficulties tracking and monitoring password changes.
- Frequently they did not include in their accounts all applicable Cyber Assets requiring procedural password changes.

9. Ensure that backup and recovery procedures are updated in a timely manner.

- CIP-009-6, Requirement R1
- Some entities failed to update their backup and recovery procedures in a timely manner.
- In some cases, entities responded to a critical event which required the entity to establish a new process that differed from their documented procedure. In these cases, the entities continued to use the new process without updating their documented process or procedure.

10. Ensure that all remediation plans and steps taken to mitigate vulnerabilities are documented.

- CIP-010-2, Requirement R3.4
- Some entities did not report any information to remediate or mitigate vulnerabilities identified in vulnerability assessments, including the planned date of completing the action plan and the execution of any remediation of mitigation items.
- NPCC has observed mitigation plans that did not include dates as well as missing documentation on the completion of addressing identified vulnerabilities.

11. Ensure that all procedures for tracking the reuse and disposal of substation assets are reviewed and updated regularly.

- CIP-011-2, Requirement R2
- Some entities were unable to demonstrate that they properly disposed of all devices removed from service at substations in accordance with the entities' documented process.
- Entities could improve their asset tracking procedures by ensuring that they maintain asset reuse and disposal logs for all substation assets.

12. Consider evaluating the security controls implemented by third parties regularly, and implement additional controls where needed when using a third party to manage BCSI.

- CIP-011-2, Requirement R1.2
- Some entities relied solely on security controls provided by third-party vendors without first verifying that these controls are sufficient.
- Failure to ensure the sufficiency of third-party vendor controls could create a risk of compromise to the BCSI if the third-party vendor controls do not provide the necessary level of protection.

Questions?

Please send all questions to cip@npcc.org