
WECC.ORG
COMPLIANCE OPEN WEBINAR
December 15, 2022, 2:00 PM MT

Compliance Open Webinar

December 15, 2022

Mailee Cook

Training and Outreach Specialist

Save the Date

- March 7–8, 2023: Board of Directors and Associated Meetings
- March 21, 2023: Virtual Reliability & Security Workshop


Grid
FUNDAMENTALS
February 21–22, 2023

Compliance Open Webinar Gets a New Name!

- Starting in 2023, the name will change to the **Reliability & Security Oversight Monthly Update**
- The new name harmonizes with the Reliability & Security Workshop and reflects the intent and purpose of these monthly webinars

Antitrust Policy

- All WECC meetings are conducted in accordance with the WECC Antitrust Policy and the NERC Antitrust Compliance Guidelines
- All participants must comply with the policy and guidelines
- This meeting is public—confidential or proprietary information should not be discussed in open session

Antitrust Policy

- This webinar is being recorded and will be posted publicly
- By participating, you give your consent for your name, voice, image, and likeness to be included in that recording
- WECC strives to ensure the information presented today is accurate and reflects the views of WECC
- However, all interpretations and positions are subject to change
- If you have any questions, please contact WECC's legal counsel

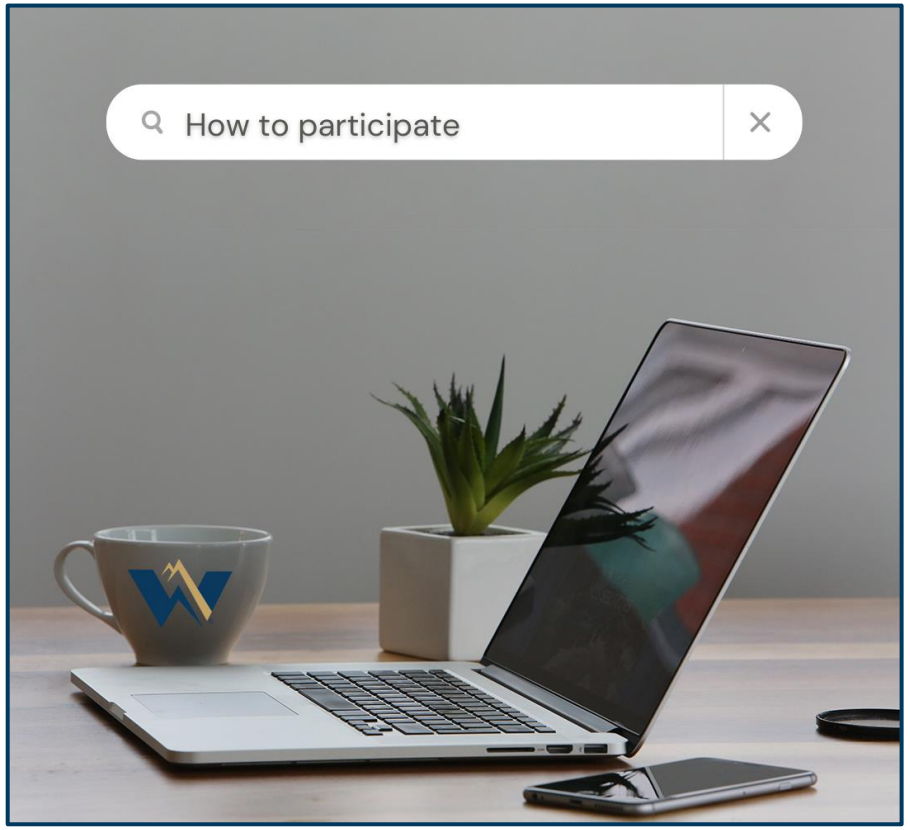
Agenda

- Align Update
  - Duane Cooke, Senior Data Analyst, Program Analysis and Administration
- Oversight Trends Report
  - Ben Aldous, Senior Compliance Analyst, Oversight Analysis & Administration

Agenda

- FERC 2022 Staff Report Lessons Learned from Commission-Led CIP Reliability Audits
  - Morgan King, Senior Technical Advisor, Entity Monitoring
- Overview of the 2023 CMEP Implementation Plan
  - Holly Peterson, Entity Monitoring Operations Lead and Senior Auditor

Participating



Send questions via chat to WECC Meetings

Use the “raise hand” feature

WECC

Align Update

December 15, 2022

Duane Cooke
Sr. Data Analyst

Audit and IRA/COP

- Plan to conduct audit and IRA/COP pilots in Align during Q1 and Q2, 2023
  - Additional audit pilots
  - Initial IRA/COP pilots
- Will notify entities participating in pilots

Canadian Entities

- Continuing to work with NERC on development and rollout of Align for Canadian entities—2023 time frame
  - Training
  - Data migration
  - webCDMS retirement

ERO Portal/CORES

- Make sure contacts are up to date
  - U.S. entities in ERO Portal/CORES
  - International entities in webCDMS
- Encourage entities to designate at least one alternate compliance contact (ACC)
  - Automated notifications go to the primary compliance contact (PCC) and any ACCs

Resources

- Questions: align@wecc.org
- Technical support: support.nerc.net
- Align homepage

WECC

Electric Reliability and Security for the West

Contact:

Duane Cooke

Sr. Data Analyst

dcooke@wecc.org

WECC

Oversight Trends Update

December 15, 2022

Ben Aldous
Sr. Analyst

Trends Update

- Data and trends highlights
- Compliance program context and comparison
- Updated quarterly
- Stakeholder partnership
- Available now on wecc.org
- Send feedback to oversight@wecc.org

WECC
Electric Reliability and Security for the West

Oversight Trends Update
Q4 2022

Oversight Trends Update Data for October 2021–September 2022

This report highlights recent Reliability and Security Oversight data and trends. WECC shares these updates to provide an interconnection-wide context for registered entity compliance programs. Data is preliminary and subject to change in future reports. Contact oversight@wecc.org with questions.

Most-Reported Requirements

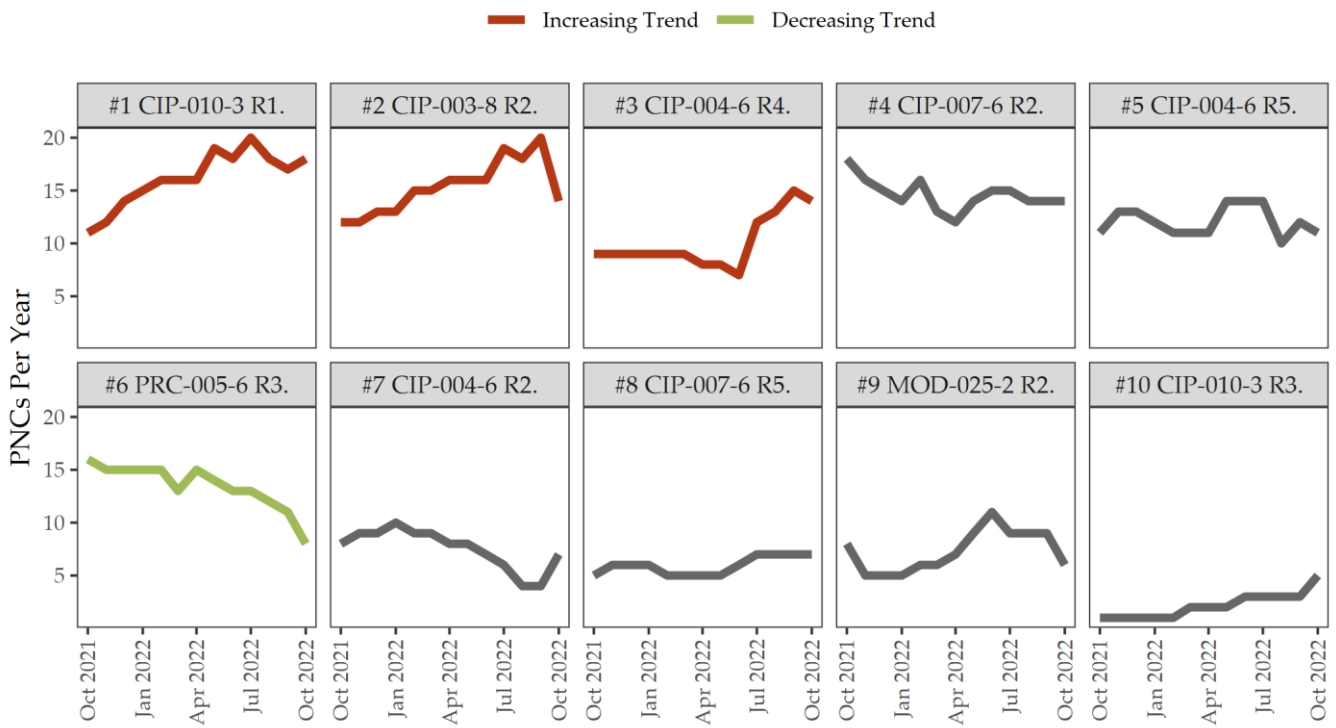
Description—These were the top 10 most self-reported requirements in the period. Charts show the trend over time in self-reported potential noncompliance (PNC) per year. Colors indicate whether the overall trend was increasing (red), decreasing (green), or unclear (gray).

Interpretation—Many factors drive self-report frequency. These include changes in the strength of industry preventive and detective internal controls, implementation of new standard versions, and issued identified in compliance programs shared by multiple entities. Change in self-report frequency alone does not indicate change in reliability but identifies areas of interest for further analysis.

155 North 400 West | Suite 200 | Salt Lake City, Utah 84103
www.wecc.org

Q4 Update

- Standards and requirements
  - Most self-reported
  - Most monitored
- Enforcement processing
  - Processing time
  - Disposition methods



WECC

Electric Reliability and Security for the West

Contact:

Ben Aldous

Sr. Analyst

baldous@wecc.org

WECC

2022 FERC Staff Report:

Lessons Learned from Commission-Led CIP Reliability Audits

December 15, 2022

Morgan King

Background

- FERC CIP audits are conducted by Office of Electric Reliability (OER) staff with assistance from Office of Enforcement (OE) staff
  - Regional Entity and NERC staff actively participate on the audits and have access to all evidence
- The Lessons Learned reports are developed by OER and Office of Energy Infrastructure Security (OEIS) staff
- Six (6) annual reports with a total of 69 lessons issued to date
  - 2022 Report (5 lessons learned)
  - 2021 Report (14 lessons learned)
  - 2020 Report (12 lessons learned)
  - 2019 Report (7 lessons learned)
  - 2018 Report (10 lessons learned)
  - 2017 Report (21 lessons learned)

Findings

- FERC staff found that, while most of the cybersecurity protection processes and procedures met the mandatory requirements of the CIP Standards, potential noncompliance and security risks remained
- FERC staff also identified practices not required by the CIP Standards that could improve security, which this report includes as voluntary cybersecurity recommendations

Standards in Lesson Learned (LL)

- CIP-003-8, Requirement R2
- CIP-007-6, Requirement R2.3 and CIP-010-4, Requirement 3.4
- CIP-007-6, Requirement R3
- CIP-010-4, Requirement R3
- CIP-010-4, Requirement R4

CIP-003-8, Requirement R2

Some entities implemented policies, procedures, and controls to protect Low Impact Cyber Systems and associated Cyber Assets that could benefit from regular re-evaluations to ensure continued effectiveness, particularly for Cyber Security Incident response and TCAs.

Cyber Security Incident Response

Some entities misinterpreted the requirement to mean Cyber Security Incident response plans are not required to be tested until 36 months from registration.

Cyber Security Incident Response (LL)

- Contrary to the NERC Rules of Procedure that require entity compliance with all applicable Reliability Standards at registration
- Entities must test its Cyber Security Incident response plans before registration and re-test them at least once every 36 calendar months

Transient Cyber Assets

Entity must identify all TCAs it manages and those managed by third parties to effectively mitigate the risk, as required by the entity's documented policy and plan associated with those TCAs managed by third parties.

Transient Cyber Assets (LL)

- Consider dedicated TCAs (e.g., laptops) and removable media (e.g., USB drives) in the operational technology environment
- Consider USB port lockdown by use of group policy orchestration toggled on/off based on requirement (Windows environment) and port locks for critical equipment

CIP-007-6, Requirement R2.3 & CIP-010-4, Requirement 3.4

Identified instances where the treatment of end-of-life (EOL) or end-of-service (EOS) BES Cyber Assets created potential security and compliance risks

CIP-007-6, Requirement R2.3 & CIP-010-4, Requirement 3.4

- Some entities:
  - Did not implement a patch management process or create dated mitigation plans for their EOL/EOS BES Cyber Assets without an applicable patch source;
  - Did not document and inventory EOL/EOS BES Cyber Assets, so were unaware of the extent of vulnerable BES Cyber Assets that had reached end of life; and
  - Did not have dated action plans to address those EOL/EOS assets as a vulnerability, as required by CIP-010 Requirement R3.4.

CIP-007-6, Requirement R2.3 & CIP-010-4, Requirement 3.4 (LL)

- Consider removing or replacing EOL/EOS hardware and software no longer supported by the vendor (NIST-800-53)
- If replacement is impossible or infeasible, entities should document, inventory, and communicate which systems and software have reached EOL/EOS and develop and implement a dated mitigation plan or a dated action plan for the vulnerabilities that these systems pose

CIP-007-6, Requirement R3

- Some entities could improve their malicious code prevention programs by:
  - Implementing additional controls and practices to detect and mitigate malware; and
  - Improving methods to deter, detect, or prevent malicious code for non-BES Cyber Assets.

CIP-007-6, Requirement R3

- Relied on controls other than antivirus to deter, detect, or prevent malware for non-Windows BES Cyber Assets—resulted in less-effective malware protection, thus exposing security gaps
  - Network controls, such as allow-listing solutions or intrusion detection/prevention solutions inconsistently configured
  - Asset hardening techniques were not implemented fully to ensure malware controls were enabled
  - Protections to deter, detect, or prevent malicious code did not exist
  - In some cases, compensating controls could not be applied due to EOL/EOS hardware or software

CIP-007-6, Requirement R3 (LL)

- Consider additional review of OT firewall logs to identify anomalies and unrecognized traffic attempting to communicate outbound
- Additional guidance in NIST Special Publication 800-83

CIP-010-4, Requirement R3

- In multiple instances, one or more of these elements were not performed during the execution of an entity's vulnerability assessments
  - Network discovery
  - Network port and service identification
  - Vulnerability review or scanning
  - Wireless review or scanning

CIP-010-4, Requirement R3 (LL)

- Entities should:
  - Consider updating policy and procedures to include network port and service identification, wireless review, and vulnerability review in vulnerability assessment processes for applicable Cyber Assets; and
  - Address, in vulnerability assessments, radio frequencies beyond Wi-Fi (e.g., 6 GHz) that may be used to send telemetry data and issue commands to field assets across significant distances.

CIP-010-4, Requirement R4

- Attestations from vendors and other third parties identified control objectives that lacked specificity on how the objectives were to be achieved
- While assurances were given that the control objectives were being met, entities did not routinely validate the existence and performance of specific measures used to mitigate risks of software vulnerabilities and malicious code

CIP-010-4, Requirement R4 (LL)

- Additional methods by which entities may achieve greater assurance beyond attestations:
  - Reviewing system owners' applicable security policies and procedures and analyzing their applicability to security requirements
  - Negotiating a "right to audit" the other party
  - Receiving and reviewing external auditor control assessments and certifications (e.g., System and Organization Controls 2 reports and International Organization for Standardization 27001 certification)

WECC

Electric Reliability and Security for the West

Contact:

Morgan King

Sr. Technical Advisor

mking@wecc.org

WECC

Overview of 2023 CMEP Implementation Plan

December 15, 2022

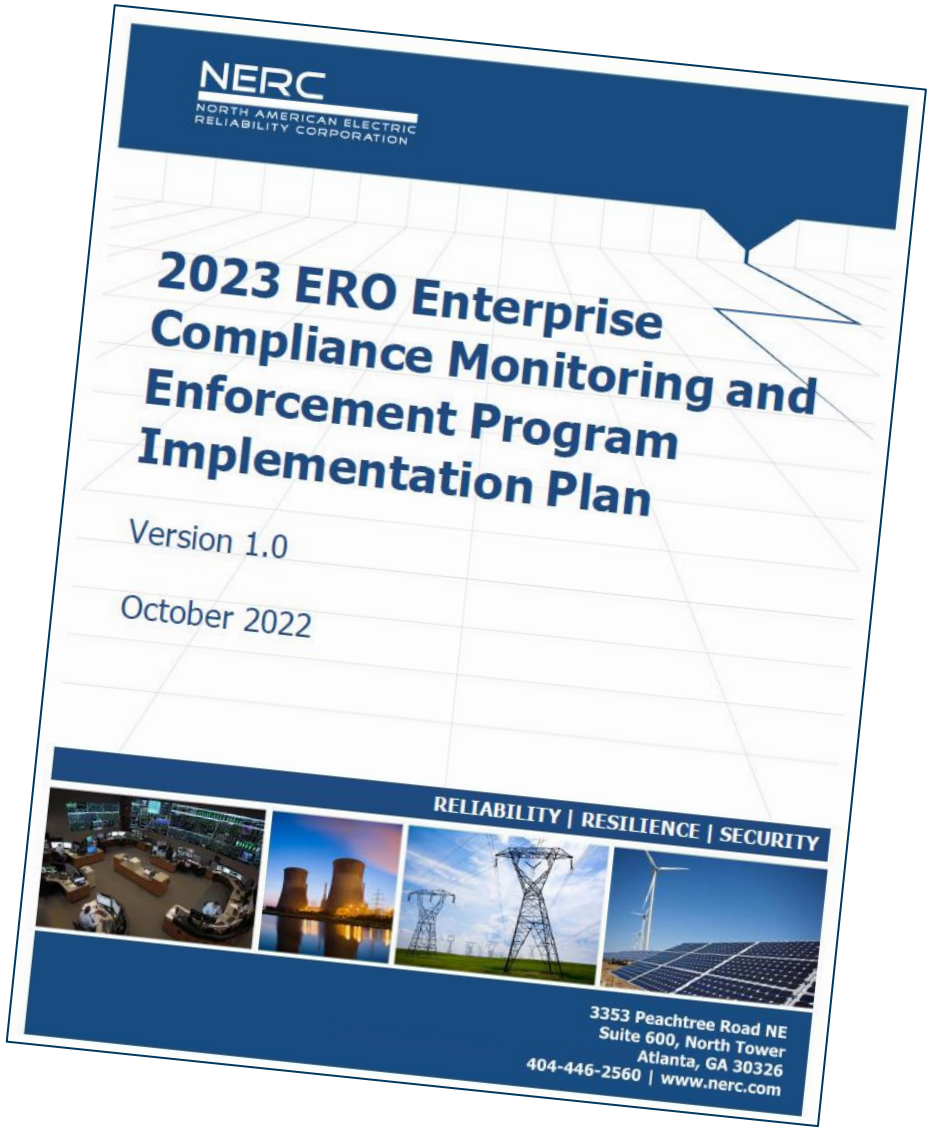
Holly Peterson, CISA, CRISC, CISSP

Entity Monitoring Operations Lead and Senior Auditor

Agenda

- Background and Purpose of CMEP IP
- Use of CMEP IP
- 2022 versus 2023 Risk Elements
  - Review of 2023 Risk Elements and Areas of Focus

[2023 CMEP IP]



What is the CMEP Implementation Plan?

- Developed to identify and prioritize the ERO Enterprise's risks for reliability of the Bulk Power System (BPS)
  - Updated annually
- Addressing risk through compliance monitoring, enforcement, outreach with industry
- Details discrete and targeted risks of the elements
  - Areas of focus relating risk elements and Requirements

What data is considered for the CMEP IP?

- NERC and six Regional Entities develop risk elements using:
  - Emerging risks
  - Compliance findings
  - Event analysis experience
  - Expert judgment
  - Reports, such as
    - ERO Reliability Risk Priorities Report
    - State of Reliability Report
    - Long-Term Reliability Assessment

Using the CMEP IP

- Focus compliance monitoring and enforcement activities
  - Prioritized Reliability Standards and Requirements to be considered for engagements
  - Enforcement may consider these risks with assessing possible noncompliance, mitigation plans, or penalties
- Communicates to entities to bring collective focus to operations and address risk
- Forms of outreach

CMEP IP and Audit Scope

- Focus will be tailored as needed
  - No expectation that every risk element or requirement is included in every engagement
- Risk elements are inputs
- Monitoring is based on characteristics, facts, and circumstances

2022 and 2023 Risk Elements

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

Remote Connectivity

- Human element of security
- Understand how entities manage the risk of remote connectivity and complexity of tasks performed by individuals

Areas of Focus

Table 3: Remote Connectivity				
Rationale	**Standard**	**Req**	**Entities for**	**Asset Types**
Remote access to Critical Infrastructure Cyber Assets introducing increased attack surface, as well as possible increased exposure.	CIP-005-7	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
Malware detection and prevention tools deployed at multiple layers (e.g., Cyber Asset, intra-Electronic Security Perimeter, and at the Electronic Access Point) are critical in maintaining a secure infrastructure.	CIP-007-6	R3	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

Supply Chain

- Continued and growing focal point
- Importance of awareness of supply chain risks

Area of Focus

Table 4: Supply Chain				
Rationale	**Standard**	**Req**	**Entities for**	**Asset Types**
Unverified software sources and the integrity of their software may introduce malware or counterfeit software.	CIP-010-4	R1	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
Mitigate risks to the reliable operation of the BES by implementing sound Supply Chain policies and procedures.	CIP-013-2	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

Incident Response

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

- Ensuring effective response to threat actions
- Example of malware targeting industrial control systems

Stability Studies

- Changing resource mix and impacts on operational and transmission planning
- Effective stability studies through modeling accuracy, protection system settings, criteria and thresholds

Areas of Focus

Table 6: Stability Studies			
Rationale	**Standard**	**Requirements**	**Entities for Attention**
Planning studies are effective in identifying system performanc e issues following both minor and major system disturbances	TPL-001-4, TPL-001-5.1	R4, R6	Transmission Planner Planning Coordinator
	CIP-014-3	R1	Transmission Owner

Inverter-Based Resources

Area of Focus

Table 7: Inverter-Based Resources			
Rationale	**Standard**	**Requirements**	**Entities for Attention**
Clear and consistent interconnection requirements for IBRs	FAC-001-3	R1, R2	Generator Owner Transmission Owner
IBRs being adequately studied	FAC-002-3	R1, R2	Generator Owner Transmission Planner Planning Coordinator
IBRs staying online when needed	PRC-024-3	R1, R2	Generator Owner

- Understand and more accurately model IBRs
- Growing number of IBRs prone to insufficient ride-through capability

Facility Ratings

- Vital to using and protecting the BES
- Importance of tracking Facility Ratings

Table 8: Facility Ratings			
Rationale	**Standard**	**Requirements**	**Entities for Attention**
Ensuring entities maintain accurate Facility Ratings	FAC-008-5	R6	Generator Owner Transmission Owner

Cold Weather Response

- Stresses the BPS and exposes weaknesses
- Nature and frequency of events and effects of grid transformation

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

Closing Thoughts

- Focus of a mature CMEP is on how the ERO Enterprise and industry proactively identify and mitigate risks to the BPS
  - Use this information to assess the risks we all want to mitigate
- CMEP IP document is a helpful resource
  - Several references throughout IP

WECC

Electric Reliability and Security for the West

Contact:

Holly Peterson, CISA, CRISC, CISSP

Entity Monitoring Operations Lead and Senior Auditor

hpeterson@wecc.org

RELIABILITY & SECURITY

Oversight Monthly Update

Formerly the Compliance Open Webinar

January 19, 2023 2:00 p.m. MT

Follow us and engage!
@weccreliability