

MRO 2023 Hybrid CMEP Conference

Understanding Risk for Reliability & Compliance

Wednesday, July 26, 2023 | 9:00 a.m. to 4:00 p.m. Central

MRO Corporate Offices, King Conference Center

St. Paul, MN 55102

And Webex



**MIDWEST
RELIABILITY
ORGANIZATION**

380 St. Peter St, Suite 800
Saint Paul, MN 55102

651-855-1760

www.MRO.net

HOSPITALITY ITEMS

Breakfast

A hot breakfast will be available from 8:00 a.m. to 9:00 a.m. in the conference center lounge. If you have any dietary restrictions, please see the registration desk or the server in the lounge.

Beverages

Hot and cold beverages will be available in the conference center, please help yourself.

Lunch

A lunch buffet will be provided. If you have any dietary restrictions, please see the registration desk or the server in the lounge. Please follow the emcee's instructions for dismissal to lunch.

Restrooms

Restrooms are located outside of the conference center, as well as on floor seven. If you choose to use a restroom on another floor, please take the elevators. The staircases only provide exit access on the first floor of the building.

First Aid

There is a first aid kit at the front desk in the reception area should you need medical or first aid supplies.

Conference Etiquette

As a courtesy to presenters and conference participants, please:

- Silence all of your electronic devices prior to sessions.
- Please defer to speakers' preferences for questions and wait for a microphone so those attending by web can hear.
- Be seated prior to the beginning of each session.

Name Badges

Please wear your name badge at all times.

Conference Evaluation

Your feedback is appreciated; a feedback form is included in this packet. Please complete the form and leave it at your seat or place it in the feedback form box at the registration table.

Luggage

Storage for any size travel luggage is available in MRO's lobby by the registration desk. Please ask MRO staff for assistance.

Lost and Found

An MRO representative will always be in the meeting room; however, personal belongings are left at your own risk. If you find or lose an item, please visit the registration desk. After the conference, please contact Lauren McClary at: lauren.mcclary@mro.net

Power and Wi-Fi

Power will be supplied at the tables. Please refrain from plugging into floor outlets to minimize the hazard from tripping. MRO's guest WIFI password can be found on the cards on the tables.

Photographs

MRO may take videos or photos at its events for use on the MRO website or in MRO publications or other media produced by MRO. MRO reserves the right to use any image taken at any event sponsored by MRO, without the express written permission of those individuals included within the photograph and/or video.

To ensure the privacy of conference attendees, images will not be identified using names or personal identifying information without the express written approval from the individual shown. If you do not wish to have your image taken for future publication, please notify MRO event staff. By participating in this MRO event or by failing to notify MRO of your desire to not have your image taken by MRO, you are agreeing to allow MRO to use your image as described.



EMERGENCY PROCEDURES

SEVERE WEATHER

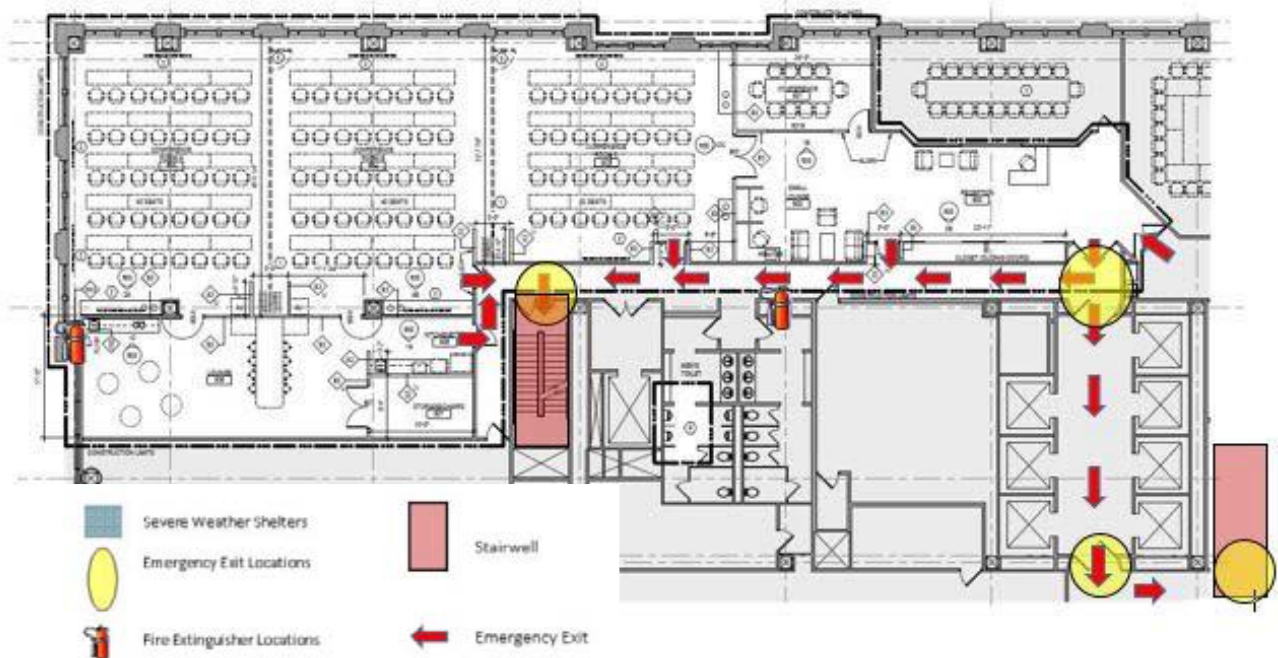
If the city of Saint Paul and/or Ramsey County sound the emergency sirens, Infor Commons building management will instruct employees to seek shelter immediately in an interior room of the building with no windows. **The building's interior corridors, stairwells, and restrooms have been designated as severe weather shelters.** Infor Commons building management will use the building's paging system to warn occupants of the need to take shelter and will also notify occupants when it's safe to return to their offices by stating "all clear."

FIRE

The Infor Commons Building is equipped with fire/strobe alarms and an automatic fire suppression and sprinkler system. Pursuant to local fire code, fire extinguishers are available for employee use in the event of an emergency. Infor Commons building management will provide instruction to building occupants in the event of a fire emergency. Fire emergencies usually do not require full evacuation.

EVACUATION

In the event the building needs to be evacuated, Infor Commons building management will notify building occupants of the need to evacuate. Use the nearest stairwell and exit the building on the ground floor (please see the evacuation map below). MRO employees and guests are asked to gather at the open Impark Lot across the street from our building on the corner of Sixth and Wabasha streets.



LOGISTICS

WebEx Login

If any help is needed logging into WebEx, please reach out to Michelle Olson at michelle.olson@mro.net.

Audio

Participants will be muted upon entry and will not be able to unmute themselves to speak.

Questions

If you have questions for a speaker, please utilize WebEx's chat feature. Please submit all questions to the "Host & Presenter". If we are unable to get all questions asked/answered during the conference, a response will be provided after the conference either directly to the requestor or through another form of outreach.

Presentations

All presentations from today's conference are available in this packet. The individual presentations and recordings from today's conference will be made available in the near future.

Feedback

Your feedback is very important to us. Please utilize the [survey link](#) also at the end of this packet, to provide your feedback.

Certificate of Attendance

If you would like to request a certificate of attendance for today's conference, please send your request to The Outreach Team at Outreach@mro.net.



AGENDA

Wednesday, July 26, 2023 | 9:00 a.m. to 4:30 p.m. Central

8:00 a.m. – 9:00 a.m.	Breakfast and Networking
9:00 a.m. – 9:20 a.m.	Conference Welcome <i>Cris Zimmerman, Manager Outreach & Stakeholder Engagement, MRO</i> <i>Emcee: Matt Caves, VP Legal & Regulatory Compliance, WFE</i> <i>CMEPAC Chair: Terri Pyle, Director, Utility Operation Compliance & NERC Compliance Officer, OG&E</i>
9:20 a.m. – 9:30 a.m.	MRO Executive: Ensuring Bulk Power System Security & Reliability <i>Lam Chung, VP and Engineer for Strategy, Innovation and Finance, MRO</i>
9:30 a.m. – 10:30 a.m.	Keynote Speaker: Reliability Risks – Cold Weather, Inverter Based Resources, Facility Ratings & Physical Security <i>Howard Gugel, VP Compliance Assurance & Registration, NERC</i>
10:30 a.m. – 10:45 a.m.	Morning Break
10:45 a.m. – 11:15 a.m.	Compliance & Enforcement Report <i>Tasha Ward, Dir, Compliance Monitoring & External Affairs Enforcement, MRO</i>
11:15 a.m. – 12:00 p.m.	Demonstrated Positive Performance <i>Jess Syring, Compliance Monitoring, Manager, CIP, MRO</i>
12:00 p.m. – 1:00 p.m.	Lunch Break
1:00 p.m. – 1:45 p.m.	Incentive Rate Treatment for Cyber Investments <i>David DeFalaise, Office of Electric Reliability (OER), FERC</i>
1:45 p.m. – 2:15 p.m.	BCSI in the Cloud (Project 2019-02) <i>Josh Powers, Compliance Supervisor, SPP</i>
2:15 p.m. – 2:45 p.m.	Virtualization (Project 2016-02) <i>Sharon Koller, Lead Compliance Strategist & CIP Sr. Manager. ATC</i>
2:45 p.m. – 3:00 p.m.	Afternoon Break
3:00 p.m. – 3:20 p.m.	CIP-014 Update <i>Sam Zewdie, Principal Compliance Engineer, O&P, MRO</i>
3:20 p.m. – 3:30 p.m.	Streamlining Standards Development Process Overview <i>Amy Casuscelli, Mgr Reliability Assurance & Risk Management, Xcel Energy</i>
3:30 p.m. – 3:50 p.m.	Cold Weather Standards Outreach <i>Brad Pabian, Mgr Maintenance, Ghent Generating Station, LG&E- KU</i>
3:50 p.m. – 4:20 p.m.	Status Report from NERC Facility Ratings Task Force (FRTF) <i>Jeremy Harris, Manager Transmission Operations Planning – Evergy</i>
4:20 p.m. – 4:30 p.m.	Conference Closing <i>Matt Caves, Emcee & Terri Pyle, CMEPAC Chair</i>



SPEAKER BIOGRAPHIES

Wednesday, July 26, 2023 | 9:00 a.m. to 4:30 p.m. Central



Amy Casuscelli

Manager of Reliability Assurance and Risk Mitigation, Xcel Energy

As Manager of Reliability Assurance and Risk Mitigation, Amy Casuscelli is responsible for Xcel Energy's NERC Compliance Program with a focus on Standards Development, Implementation, and emerging issues.

Ms. Casuscelli initially joined Xcel Energy in the Supply Chain organization in 2009. In 2013 she transitioned to the Federal Regulatory Affairs department and has held various positions performing NERC Compliance functions.

Over the years Ms. Casuscelli has been involved with various committees and stakeholder groups and is the current Chair of the NERC Standards Committee.

She is a graduate of the University of Minnesota with a Bachelor of Arts in Political Science and Master of Science in Security Technologies.

Contact Amy: Amy.R.Casuscelli@xcelenergy.com



Brad Pabian

Manager of Maintenance, Ghent Generating Station

Brad Pabian is a graduate of the University of Kentucky with bachelor's and master's degrees in mechanical engineering. He has worked with Louisville Gas & Electric and Kentucky Utilities for 15 years in various roles of power plant engineering and maintenance leadership at the E. W. Brown Generating Station, Ghent Generating Station, and in the company's corporate generation engineering group.

He currently serves as the Maintenance Manager at the Ghent Station, a 4-unit 2,000 MW coal-fired facility. Outside of work, he enjoys being part of the technology team at his church, flying and all things related to general aviation, and spending time with his wife and daughter.

Contact Brad: Brad.pabian@lge-ku.com



Cris Zimmerman

Manager, Outreach and Stakeholder Engagement, MRO



Cris Zimmerman is the Manager, Outreach and Stakeholder Engagement for Midwest Reliability Organization (MRO). Cris has been in the newly created Outreach Manager role since May of 2022. Prior to MRO, Cris was with Xcel Energy for 31 years, where he held several management positions. In his most recent role with Xcel Energy, he was Director, Operations Technical Training. Cris's experience has spanned many sectors of the electric utility industry including nuclear, coal, gas, wind, solar power production, environmental services, and electric transmission and distribution. The majority of his time was spent supporting technical, compliance and safety training.

Cris holds a Bachelor of Science degree in Education from Plymouth State University and a Mini MBA for Environmental Professionals from the University of St. Thomas. Cris has also held certifications as a nationally certified Emergency Medical Technician (EMT) and State of Minnesota Certified Firefighter II. Cris spent seven years as an on-call firefighter/EMT for the city of Woodbury, MN.

Contact Cris: Cris.Zimmerman@mro.net

David DeFalaize

Energy Infrastructure and Cybersecurity Advisor, FERC



David DeFalaize is an Energy Infrastructure and Cybersecurity Advisor in the Office of Electric Reliability at Federal Energy Regulatory Commission (FERC). David has worked at FERC for 11 years and was the supervisor overseeing the Commission processing of Order No. 791 (CIP Version 5) and Order No. 822 (Revisions to CIP v5).

Prior to working at FERC, David spent 10 years as a civilian with the US Navy overseeing development of SCADA systems for pipelines and fuel storage. Before that David did development for and worked in data centers in the predecessor to what would become "Data Center Alley" in Northern Virginia. However, somewhere along the line David had screwed up as the original plan with his degree in Mathematics was to become an actuary, which US News & World Report said was the best job to have in the 1990's for quality of life.

Contact Chuck: David.DeFalaize@ferc.gov





Howard Gugel

Vice President, Compliance Assurance and Registration, NERC

Howard Gugel is the vice president of Compliance Assurance and Registration at NERC. In this role he is responsible directing programs and processes to monitor, review, and evaluate program effectiveness of Electric Reliability Organization (ERO) Enterprise implementation of risk-based compliance monitoring and adherence to the NERC Rules of Procedure, Compliance Monitoring and Enforcement Program, and approved delegation agreements. He is also responsible for overseeing the ERO's organization registration and certification process.

In 2022, Mr. Gugel was appointed to the Department of Energy's Electric Advisory Committee by the Secretary of Energy. He also serves on the North American Energy Standards Board. Mr. Gugel has more than 34 years of experience in the electric utility industry, including management experience in transmission planning, operations, and energy marketing. He has worked for two investor-owned utilities, a rural electric cooperative, and an energy marketing firm.

Mr. Gugel earned his bachelor's and master's degree in Electrical Engineering from the University of Missouri – Rolla. He is a licensed professional engineer in the state of Missouri.

Contact Désirée: howard.gugel@nerc.net



Jeremy Harris

Manager Transmission Operations Planning – Evergy

Jeremy Harris is the Manager of Transmission Operations Planning for Evergy. Jeremy has over 12 years of experience in Transmission Planning and System Operations. Jeremy is a member of the NERC Facility Ratings Task Force, the NATF Facility Ratings project, the NATF FERC Order 881 Working Group, SPP Operations Reliability Working Group, and previous member and vice chair of the SPP Model Development Advisory Group.

Jeremy received his BSEE degree from Kansas State University in 2010.

Contact Désirée: Jeremy.Harris@evergy.com





Jessica Syring

Compliance Monitoring Manager, CIP

Jessica Syring joined MRO in December 2015 as a CIP Compliance Engineer. Ms. Syring transitioned to the role of Compliance Monitoring Manager, CIP, in January 2020.

Ms. Syring joined the MRO compliance team after working nine and a half years for Open Systems International, Inc. (OSI). While at OSI she assisted with EMS SCADA server system design, implementation, training, testing, and commissioning. She also assisted with technical troubleshooting of power system critical issues as well as upgrading systems with vendor software.

Ms. Syring is a graduate of the University of Minnesota, with a Bachelor of Science degree in Computer Engineering.

Contact Jess: jess.syring@mro.net



Josh Powers

Compliance Supervisor, Southwest Power Pool

Josh Powers joined the Compliance Group at Southwest Power Pool (SPP) in March 2018 as a Senior CIP Compliance Specialist and has since transitioned to the role of Lead CMEP Specialist. SPP is one of nine independent system operators (ISOs) and regional transmission organizations (RTOs) in North America, located in Little Rock, AR. Mr. Powers focuses on promoting and facilitating a just culture of compliance at SPP that maximizes reliability and security of the Bulk Electric System while helping to minimize the risk of potential noncompliance with the NERC Reliability Standards throughout the organization.

Prior to joining SPP, Mr. Powers worked for URS Corporation and Bechtel Corporation for a combined 11 years at chemical demilitarization facilities located in Pine Bluff, AR, and Richmond, KY. His duties include DoD compliance, process and business analysis, and technical publications, including serving in a supervisory role for 4 years. Mr. Powers was also a recipient of the URS 2011 Chairman's Award given to a select group of individuals who led the URS Federal Services project of the year (Pine Bluff Chemical Agent Disposal Facility).

Mr. Powers attended and graduated *magna cum laude* from the University of Arkansas at Little Rock, earning bachelor's degrees in professional and technical writing as well as international studies in 2006. In addition, Josh has been engaged in many industry groups and teams since joining SPP.

Contact Josh: jpowers@spp.org





Lam Chung

Vice President and Engineer for Strategy, Innovation and Finance, MRO

Lam Chung joined MRO in September 2019 as vice president and engineer for strategy, innovation, and finance. Previously with Manitoba Hydro, Chung has more than 20 years of experience in the electric utility sector, responsible for progressively senior roles in engineering and design, operations, Independent System Operator/Regional Transmission Organization markets, regulatory affairs, and compliance.

He has experience at the national and international levels, having served on the NERC Member Representatives Committee, which provides policy input and elects individuals to serve on the NERC Board of Trustees, and the Canadian Electricity Association, serving as vice chair of the Electric Regulatory Advisory Committee. He has also collaborated on work with the United Nations Office for Project Services.

Chung earned both his Bachelor of Science in Electrical Engineering and his Masters of Business Administration degrees from the University of Manitoba and is a licensed Professional Engineer.

Contact Lam: lam.chung@mro.net



Matt Caves

Senior Manager, Legal & Regulatory Compliance, Western Farmers Electric Cooperative

Matt Caves currently serves as the Corporate Compliance Officer and Senior Manager of Legal and Regulatory Compliance for Western Farmers Electric Cooperative (WFEC), a generation and transmission cooperative located in Anadarko, Oklahoma. Prior to joining WFEC, Matt spent almost 15 years as a state regulator and in private practice handling a wide variety of regulatory compliance, permitting, enforcement and litigation issues.

Matt is an active member of the Reliability Compliance Working Group (RCWG), Markets and Operations Policy Committee (MOPC), and Strategic Planning Committee (SPC) of the Southwest Power Pool (SPP). Matt obtained his Bachelor of Science degree in Wildlife and Fisheries Ecology from Oklahoma State University and his Juris Doctorate degree from The University of Oklahoma, College of Law.

Contact Matt: matt.caves@wfec.com





Samuel S. Zewdie

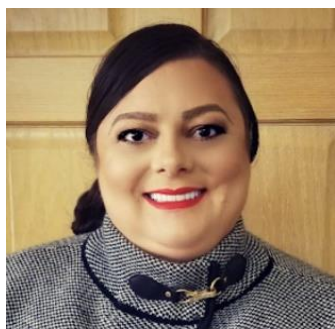
Principal Compliance Engineer, O&P, MRO

Samuel Zewdie joined MRO in September 2013 as a Staff Engineer and became a Compliance Engineer in May 2018. Mr. Zewdie transitioned to the role of Senior Compliance Engineer in January 2020 and in 2023 he was promoted to Principal Compliance Engineer.

Prior to joining MRO, Mr. Zewdie worked for MAPPCOR as a Transmission Planning Engineer. While at MAPPCOR, he worked on regional assessment, planning studies, voltage stability studies, transfer studies, and design of UFLS program for the MAPP region. Mr. Zewdie also briefly worked for Great River Energy where he focused on substation bus bar analysis, PSS/E model building and areal planning.

Mr. Zewdie is a graduate of the University of Minnesota with a Bachelor of Science and a Master of Science in Electrical Engineering with minor in Industrial Engineering. He is a registered professional engineer (PE) in the state of Minnesota and member of Eta Kappa Nu - HKN (National EE Honor Society) and IEEE.

Contact Sam: Sam.Zewdie@mro.net



Sharon Koller

Lead Compliance Strategist & CIP Sr. Manager, ATC

Sharon Koller, Lead Compliance Strategist & CIP Sr. Manager, joined ATC in 2013 and has 25 years' experience in the utility industry. Koller is committed to contributing to safe, resilient, and reliable operation of the BES through implementation of sound security practices and internal controls. Koller serves in an internal assurance, oversight, and governance role providing CIP interpretation and advisory services; management of potential non-compliance; operational alignment of centralized programs, metrics, and tools with ATC's reliability and security strategy. Koller is a current member of the 2016-02 CIP Standards Drafting Team, Vice Chair of 2022-05, formerly served on 2018-02, 2019-02, and 2019-03, was a member of the MRO CMEP Advisory Council from 2019-2021, and an MRO HERO award recipient in 2021. Prior to ATC, Koller served Alliant Energy for 16 years, in various technical, compliance, project, and program management capacities.

Contact Sharon: skoller@atcllc.com





Tasha Ward

Director of Enforcement and External Affairs, MRO

Tasha Ward is the Director of Enforcement and External Affairs for the Midwest Reliability Organization (MRO). Mrs. Ward is responsible for the enforcement of the Reliability Standards as detailed in the NERC Compliance Monitoring and Enforcement Program (CMEP) within the MRO region. Mrs. Ward is also responsible for MRO's External Affairs within the United States. Mrs. Ward joined MRO in October 2019.

Prior to joining MRO, Mrs. Ward served as the Lead Compliance Monitoring and Enforcement Specialist at Southwest Power Pool, a member-based organization that oversees the bulk electric grid and wholesale power market for 14 states. A familiar face to the Electric Reliability Organization (ERO), Mrs. Ward also served as a Senior Enforcement Attorney for the Southwest Power Pool Regional Entity (SPP RE) from 2009 until 2015 and rejoined in 2017 until dissolution in 2018. During her gap year with the SPP RE, Mrs. Ward contracted with the SERC Reliability Corporation and taught computer courses to students in 1st through 8th grades. Early in her career, Mrs. Ward was a law clerk at the Arkansas Supreme Court for the Honorable Justice Jim Gunter and served as Associate Executive Director at the Arkansas Bar Association.

Mrs. Ward graduated with a Bachelor of Science from the University of Central Arkansas located in Conway, AR and received her Doctor of Jurisprudence (J.D.) from the University of Arkansas at Little Rock Bowen School of Law in Little Rock, AR. She is licensed to practice law in Arkansas and Texas and is a Certified Compliance and Ethics Professional. She holds a Women in Leadership Certificate from Minnesota State University-Mankato. She is a member of the Texas Bar Association, the Energy Bar Association, the Society of Corporate Compliance and Ethics, and an Advisory Board Member of the Women in Leadership program at Minnesota State University-Mankato.

Contact Tasha: tasha.ward@mro.net





Terri Pyle,

*Director Utility Operation Compliance, Oklahoma Gas and Electric,
MRO CMEPAC Chair*

Ms. Pyle is currently the Director of Utility Operational Compliance at Oklahoma Gas and Electric Co (OG&E) where she is responsible for the overall development and execution of OG&E's NERC Compliance Program since 2011. Ms. Pyle also holds the roles of NERC Compliance Officer and NERC CIP Senior Manager for OG&E.

Ms. Pyle has been with OG&E since 2011 and is responsible for leading OG&E's NERC Compliance Program and directing the activities of (1) monitoring new and changing Reliability Standards, (2) partnering with the affected business units to develop comment and ballot positions, (3) assessing the potential impacts to the business, (4) implementing the associated risk management and internal controls programs, (5) assuring compliance to the Reliability Standards and (6) audit, enforcement, and mitigation activities. Additional areas of responsibility include Business Resiliency and Continuity (2022 to present) and the Compliance Contact for the Executive Response Team.

Ms. Pyle also serves as OG&E's liaison for all NERC Compliance matters with the ERO and participates and holds leadership roles in industry and trade organizations; leadership roles include serving as the Chair of the MRO CMEP Advisory Council (2022), Vice Chair of the MRO CMEP Advisory Council (2020-2021), participant in MRO NERC Standards Review Forum (NSRF), voting member of the SPP Reliability Compliance Advisory Group (2016 to present), NATF Risk, Controls, Compliance Core Team member (2019 to present), the EEI REAC representative (since 2018) and voting member of the NERC Standards Committee (2021 to present).

Prior to joining OG&E, Ms. Pyle served as the Compliance Manager for Oklahoma Municipal Power Authority (OMPA) from 2007 – 2011 and responsible for all compliance matters related to Safety, Environmental, and NERC. Prior to that she served as the Manager of Environmental Compliance for Delta Faucet Company facilities in the U.S. and Asia.

Contact Terri: pyleta@oge.com



MRO DISCLAIMER

Midwest Reliability Organization (MRO) is committed to providing outreach, training, and non-binding guidance to industry stakeholders on important industry topics. Subject Matter Experts (SMEs) from MRO's organizational groups and the industry may develop materials, including presentations, provided as a part of the event. The views expressed in the event materials are those of the SMEs and do not necessarily express the opinions and views of MRO.



PRESENTATIONS

All presentations for today's conference are included in order of presentation. Some presentations may have changed slightly after the print deadline.





MIDWEST
RELIABILITY
ORGANIZATION

Welcome to the 2023 Hybrid CMEP Conference

July 26, 2023

Cris Zimmerman Manager, Outreach &
Stakeholder Engagement

CLARITY

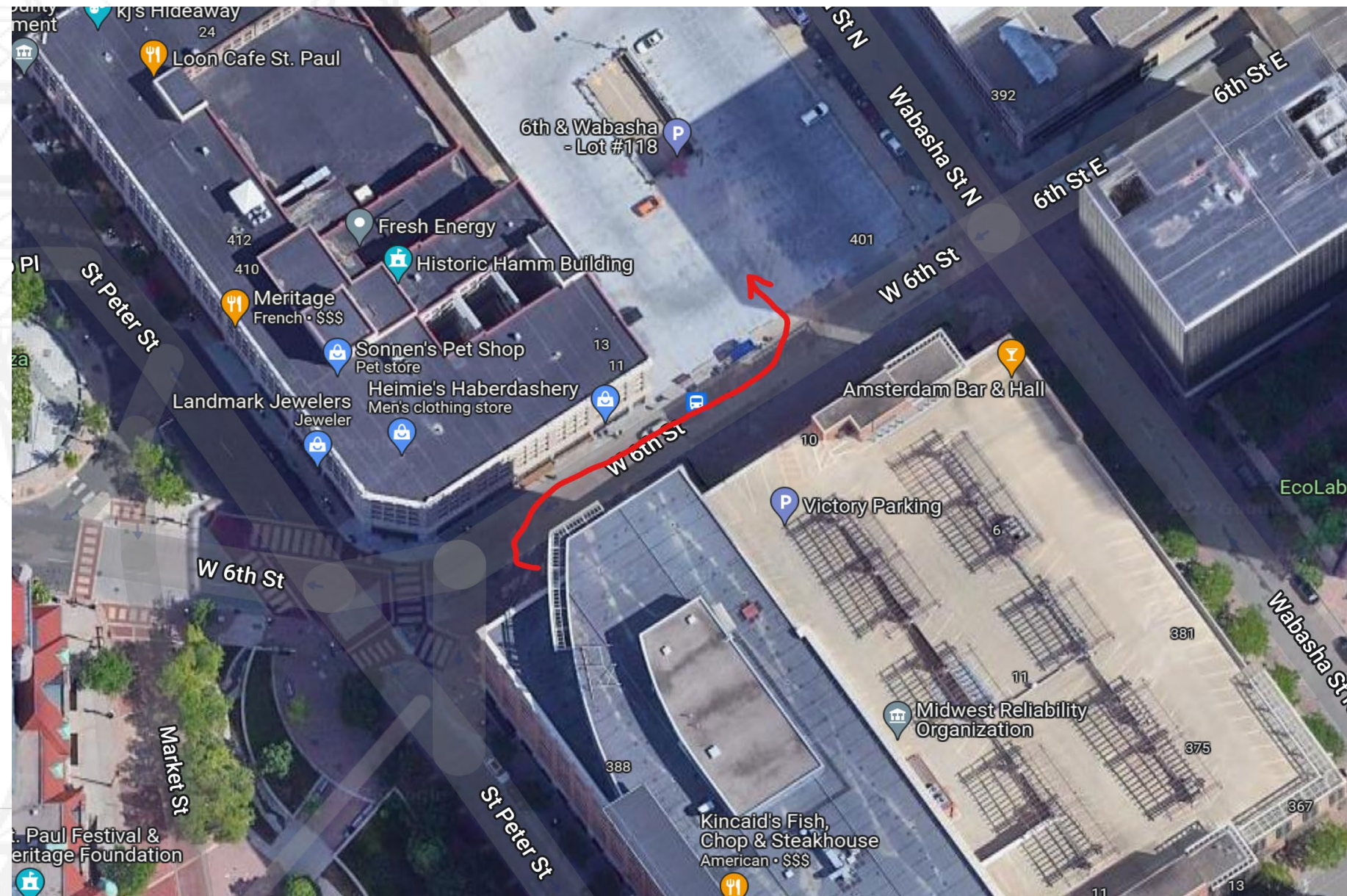
ASSURANCE

RESULTS

MRO Logistics, Safety & E-Plan

- **Safety – First Aid, CPR and AED**
- **Food and beverages**
- **Restrooms**
- **Emergency plan – severe weather/evacuation**

Evacuation route & accountability location 6th St & Wabasha St





HERO

HIGHLY EFFECTIVE RELIABILITY ORGANIZATION

FIVE BASIC PRINCIPLES:

1. **Preoccupation with failure**

Attention on close calls and near misses (“being lucky vs. being good”); focus more on failures rather than successes.

2. **Reluctance to simplify interpretations**

Solid “root cause” analysis practices.

3. **Sensitivity to operations**

Situational awareness and carefully designed change management processes.

4. **Commitment to Resilience**

Resources are continually devoted to corrective action plans and training.

5. **Deference to Expertise**

Listen to your experts on the front lines (ex. authority follows expertise).

Annual HERO Award

Nominate Someone
Today!



MIDWEST
RELIABILITY
ORGANIZATION

www.mro.net/about/hero/



HERO

HIGHLY EFFECTIVE RELIABILITY ORGANIZATION



Upcoming Event Dates

- **Aug 29th 10am – 11am IT/OT Convergence Security Webinar – Doug Peterchuck, OPPD**
- **10th Annual MRO Security Hybrid Conference – Sept 26-28, 2023 Oklahoma City, OK – Sheraton Hotel**

2023 CMEP Conference Survey



<https://www.surveymonkey.com/r/JVM9VBQ>



CLARITY

ASSURANCE

RESULTS

Disclaimer for organizational group hosted events or materials

Midwest Reliability Organization (MRO) is committed to providing outreach, training, and non-binding guidance to industry stakeholders on important industry topics. Subject Matter Experts (SMEs) from MRO's organizational groups and the industry may develop materials, including presentations, provided as a part of the event. The views expressed in the materials are those of the SMEs and do not necessarily express the opinions and views of MRO.





MIDWEST
RELIABILITY
ORGANIZATION

Welcome from the CMEP AC

Terri Pyle, CMEP AC Chair
NERC Compliance Officer, OG&E

2023 MRO CMEP Hybrid Conference

July 26, 2023

CLARITY

ASSURANCE

RESULTS

CMEP Advisory Council

Purpose

The MRO Compliance Monitoring and Enforcement Program Advisory Council (MRO CMEPAC) is an MRO Organizational Group that provides advice and counsel to MRO's Board of Directors (board), the board's Organizational Group Oversight Committee (OGOC), staff, members and registered entities on topics such as the development, retirement, and application of NERC Reliability Standards, risk assessment, compliance monitoring, and the enforcement of applicable standards. The MRO CMEPAC increases outreach and awareness in these key areas.



CMEPAC Initiatives

1. Requirement Specific RFI – CIP-007 R2, FAC-008 R6
2. RRA and associated NERC Reliability Standards
3. Newly Enforceable Standards
4. Readiness Assessment – EOP-012-1 R2





MIDWEST
RELIABILITY
ORGANIZATION

Theme: Understanding Risk for Reliability & Compliance

CLARITY

ASSURANCE

RESULTS



MIDWEST
RELIABILITY
ORGANIZATION

Ensuring Bulk Power System Security and Reliability

Lam Chung

MRO VP and Engineer for Strategy, Innovation, and Finance

2023 MRO CMEP Hybrid Conference

July 26, 2023

CLARITY

ASSURANCE

RESULTS

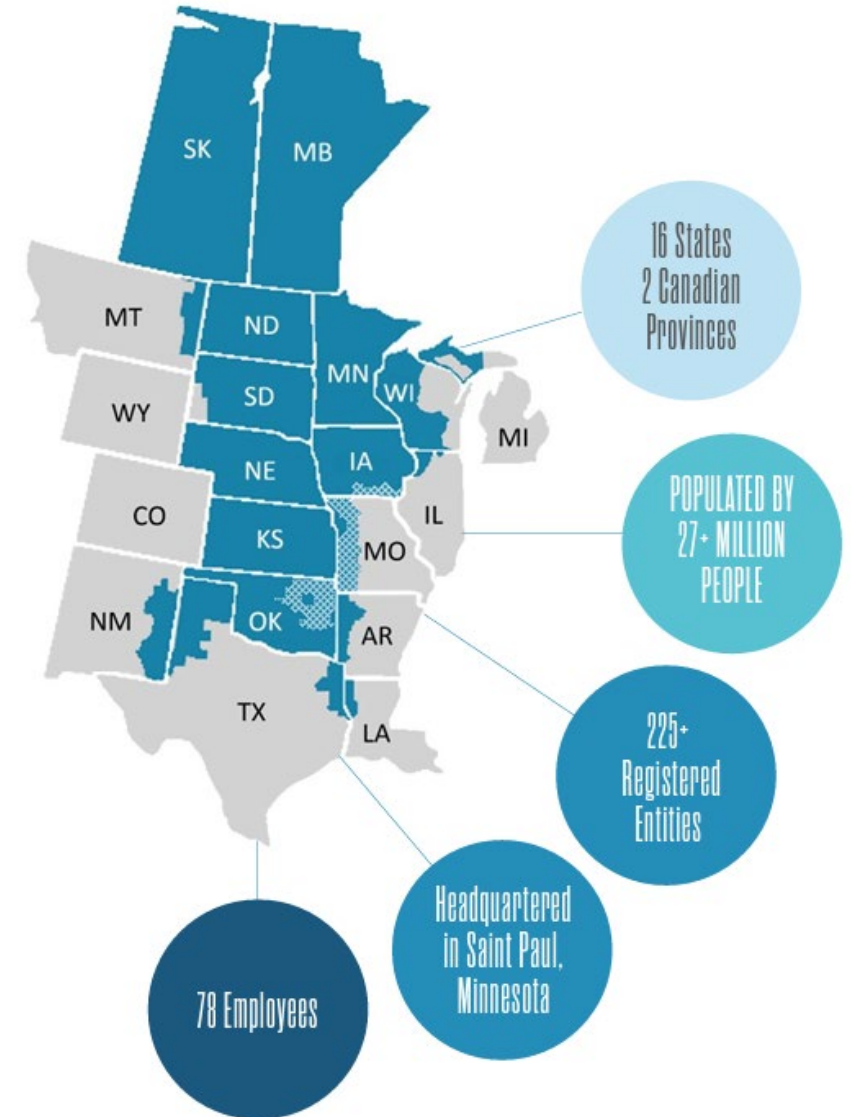
Vision and Mission

VISION

**A highly
reliable and
secure North
American
bulk power
system**

MISSION

**To identify, prioritize
and assure effective
and efficient
mitigation of risks to
the reliability and
security of the North
American bulk power
system by promoting
Highly Effective
Reliability
Organizations
(HEROs)**



CLARITY

ASSURANCE

RESULT



Broad and Collaborative Partnerships



WITH ERO
COLLABORATORS



WITH REGISTERED
ENTITIES



WITH STATE
REGULATORS



WITH CANADIAN
PARTNERS



CLARITY

ASSURANCE

RESULTS

STRATEGIC PLAN 2022-24

A highly reliable and secure North American bulk power system



PEOPLE

1 Ensure that MRO remains an innovative, resilient, and high-performing organization with an increased emphasis on leadership development and culture.

1. Ensure continuous learning, growth, and career development opportunities.
2. Foster a culture of diversity, equity, inclusion, honesty, and trust through constructive feedback, empowerment, and clarity of roles.
3. Promote opportunities for crossdepartmental and inter-ERO collaboration.
4. Formalize processes to ensure continuity of leadership and a skilled and engaged workforce.

2

Drive operational excellence throughout MRO in all processes and procedures, while emphasizing effectiveness and efficiency.

1. Focus on identifying, assessing, and mitigating corporate risks and ensure expenditure of resources are prioritized and appropriately deployed.
2. Foster a culture of continued improvement and innovation through forward thinking and futuristic visioning.
3. Leverage KPIs to measure operational effectiveness.
4. Identify and implement processes to assess and prioritize work.



PARTNERSHIPS

3

Develop a nimble, adaptive, and collaborative culture that allows us to carry out our mission as a trusted and valued member of the ERO Enterprise.

1. Focus on advanced methods for identifying, assessing, and actively mitigating new and emerging risks to the BPS and ensure resources are deployed appropriately.
2. Lead and support ERO transformation efforts.
3. Expand collaborative relationships with federal, state, and provincial regulators, independent system operators, industry leadership, and the broader reliability and security ecosystem.
4. Ensure security and confidentiality of our partners' data and information.
5. Increase capability to support mitigation of increasing frequency and sophistication of cyber risks for corporate and industry (ransomware phishing, vulnerabilities, etc.).
6. Be a trusted leader in providing premier and cutting edge outreach to our stakeholders.



PROCESSES

MRO Budget Process Summary

1

Staff develops a “bottoms-up/zero-based” preliminary budget developed with program managers and executives

“Tops-down” expectations from president and CEO

Reconcile “bottoms-up” to “tops-down”

2

Present budget to MRO FAC

Detailed review and justification of all line items, contracts, etc.

MRO FAC hosts board conference call to review budget and recommend approval

3

Budget is circulated for comment to all MRO stakeholders

Budget is considered and approved at second quarter MRO board meeting

Approved budget is submitted to NERC

4

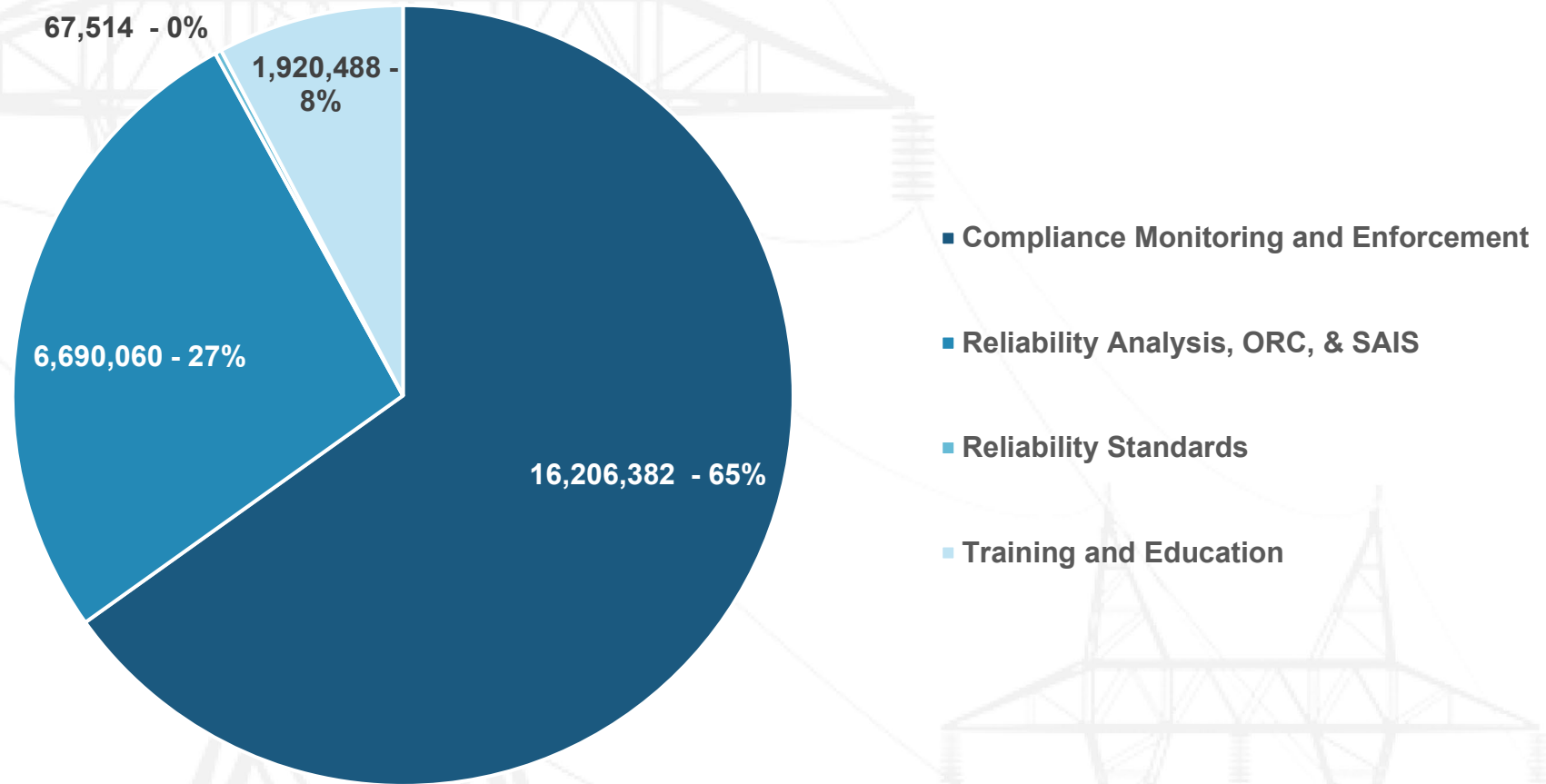
NERC posts all Regions’ and NERC budget for industry comment

NERC board approves (or may have questions, concerns to address)

Final approval of NERC and RE budgets are filed with FERC



2024 Budget by Program Area



MRO Value Proposition

Risk-Informed Products/Services

- **Seasonal and long-term reliability assessments**
- **Annual reports on state of reliability and reliability risk priorities**
- **Risk-based compliance monitoring and enforcement processes**
- **Coordinated grid security exercises**
- **Event and performance analysis and lessons learned**
- **Entity assistance visits like the generator weatherization program**
- **Outreach and training**
 - 4 major conferences annually
 - Webinars and in-person events
 - Newsletter articles

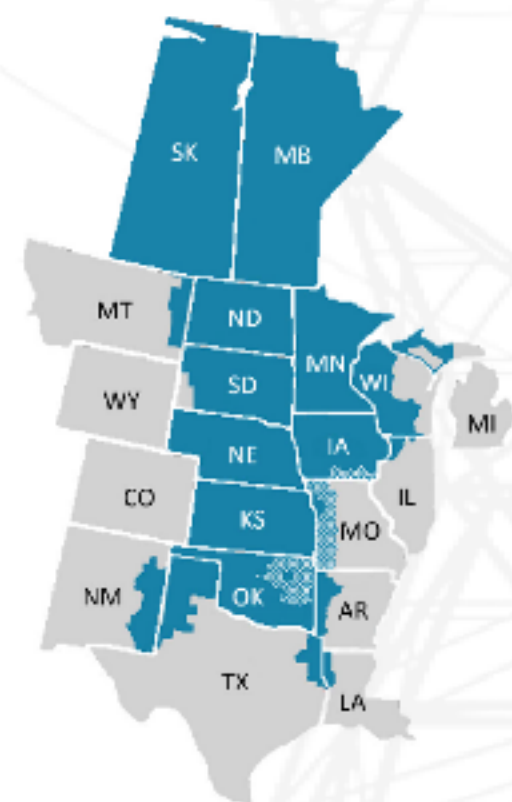




MRO 2023 Regional Risk Assessment

Top risks to the reliable and secure operation of the North American bulk power system in MRO's regional footprint.

Territory



About Us

As part of the [ERO Enterprise](#), MRO is committed to a shared mission to identify, prioritize and assure effective and efficient mitigation of risks to the reliability and security of the North American bulk power system in its regional footprint.

Read more at www.MRO.net

MRO Reliability Risk Matrix: Risk Rankings

Consequence / Impact (C)		Likelihood (L)				
		L1	L2	L3	L4	L5
		Very Unlikely	Unlikely	Possible	Likely	Almost Certain
C5	Severe					
C4	Major				4,5,6,16	
C3	Moderate		2	9,12,13	1	
C2	Minor			3,7,8,10,14,17	15	
C1	Negligible			11		



Top risks are reflected in orange above and described below. A full list of risks assessed can be found in the final report.

Key Findings: Top Reliability and Security Risks in MRO's Territory

Model Assumptions



RISK 1. Assumptions used in bulk power models to plan and operate the grid have not accounted for the rapid increase in inverter-based and distributed energy resources, challenging industry's ability to accurately assess current and future system characteristics.

Planning Reserves



RISK 4. Traditional methods to calculate Planning Reserve Margin are inadequate to properly plan for the generation capacity needed to meet increasingly uncertain system operations, especially during extreme weather events.

Energy Reliability



RISK 5. Increased uncertainty from changing energy supply and customer demand challenge the grid's ability to meet load for all hours of the year. There is no comprehensive planning that assesses assurance of available energy and fuel sources over all time periods to maintain grid reliability.

Generation Unavailability



RISK 6. Generation availability assumed during cold weather, particularly in the southern U.S., has been shown to be unrealistically high due to a lack of generation winterization and natural gas curtailments.

Transmission Line Ratings



RISK 12. Use of constant overhead transmission line ratings year-round (non-seasonal) limits available transmission capacity and leads to inefficient real-time decisions when system conditions deviate from assumptions that drive rating calculations, such as cooler temperatures or during emergency operations.

Insider Threats



RISK 9. Employees or contractors using their knowledge and authorized access of critical systems to do harm to the bulk power system is a continued, substantial threat to organizations and the reliability of the grid.

Malware/Ransomware



RISK 13. Phishing attacks can introduce malware or ransomware to corporate IT systems, which can impact critical systems necessary for reliable bulk power system operations through direct or in-direct connections those systems have to IT networks.

Supply Chain Compromise



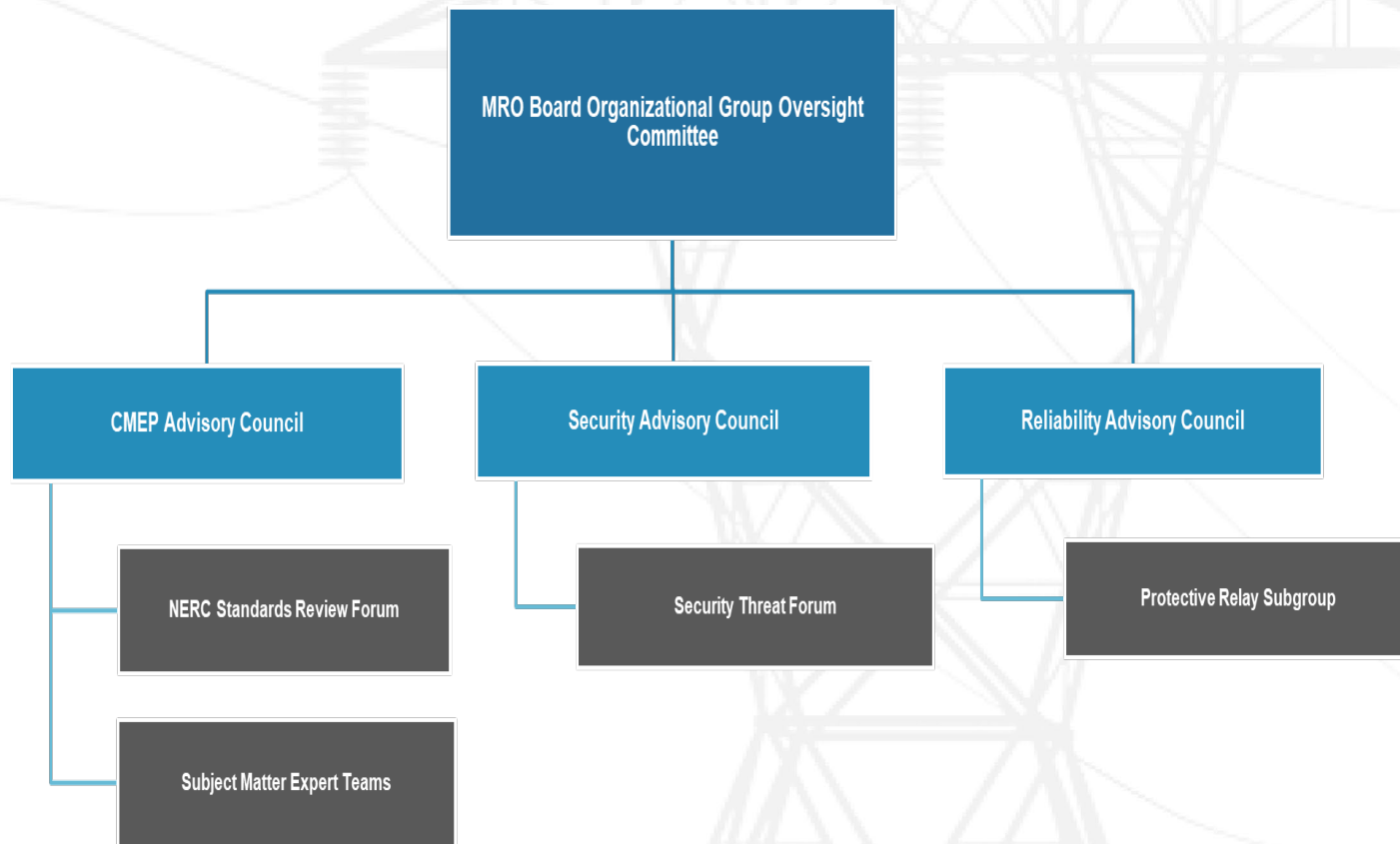
RISK 16. A cyber security event carried out through the vendor supply chain can broadly impact bulk power system reliability, especially where the vendor is a market leader providing systems used for system operation.

Assessment Overview

- Extreme weather, consumer demand, and changes in technology and generation resources continue to present a rapidly increasing number of challenges to grid planners and operators. Physical and cyber security risks also continue to evolve at an unprecedented pace.
- MRO's annual *Regional Risk Assessment* considers continent-wide risks to reliability and security of the North American bulk power system and determines which are more likely to occur and would have a higher impact in MRO's region.
- This report is focused on risk identification, prioritization and mitigation and highlights for industry the priorities needed to collaboratively address these challenges. It also serves to inform key decision makers of challenges the industry faces and the policies and regulations that will help define a variety of proposed solutions.

READ MRO'S [2023 REGIONAL RISK ASSESSMENT](#)

Sharing Information and Best Practices



Continuous Improvement and Innovation Program

- Highlight industry efforts to:
 - Implement high standards of operational excellence
 - promote a culture of continuous improvement
 - develop innovative solutions to complex risk



IDENTIFICATION AND MITIGATION OF SIGNIFICANT RISKS TO RELIABILITY:

“ EXISTING AND EMERGING LANDSCAPE OF RISKS ”

TRANSMISSION CHALLENGES: AND NEEDS



BALANCING CONFIDENTIALITY
AND TRANSPARENCY



- USE OF RAS + SPS
- INTEGRATE MORE DATA AND SOFTWARE APPLICATIONS FOR FUTURE ADAPTATION

CALIFORNIA (+WESTERN STATES)

- CHALLENGES:
- DUCK CURVE
 - VOLTAGE CONTROL
 - WILD FIRES

“ 3 D ” GRID

DECENTRALIZATION

- Diversifying energy sources, thinking regionally

DECARBONIZING

- eliminating coal, replace w/ HYDRO + NUCLEAR

DIGITALIZATION

- embracing new technology / communication / collaboration

- STRATEGY:
- address TRANSMISSION needs
 - Create + validate models



CISA
CYBERSECURITY AND
INFRASTRUCTURE
SECURITY AGENCY



MAINTAINING
PHYSICAL
+
CYBER
SECURITY

MAJOR THREATS

- 1 - DEPENDENCE ON SINGLE RESOURCE
- 1 - DRONES
- 1 - LARGE NATIONAL GATHERINGS + EVENTS
- 1 - FOREIGN MANUFACTURED DRONES (DATA LOSS)
- 1 - CHINA - TAKING DATA,

SOLUTIONS

- INFO-SHARING
- “CYBER HYGIENE”
- BUILDING RESILIENCE
- EXERCISE INCIDENT RESPONSE

IMPROVEMENTS

- COMMUNICATION
- SMART TECH
- PUBLIC / PRIVATE PARTNERSHIPS

WHAT IS SHARED
THROUGH DEVICES
+ DATA?

Q+A TOPICS: SUPPLY CHAIN

- 1. VENDOR RESPONSE
- DOE COLLAB w/

INTERNET CONTROL / MONITORING

- 1. NEW AGGREGATORS
- CHINA + RUSSIA BUILDING OWN INTERNET - BREAKING OFF

the sketch effect

It Takes a Village



NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Reliability Risks

Howard Gugel, Vice President of Compliance Assurance and Registration
MRO CMEP Conference
July 26, 2023

RELIABILITY | RESILIENCE | SECURITY



- Cold Weather
- Inverter-Based Resources
- Facility Ratings
- Physical Security

- Unplanned generation losses exceeding 70,000 MW
- Firm load shed exceeding 5,000 MW
- Load forecasts were off significantly
- Dry natural gas production decreased
- Issues in production, processing, and pipeline for natural gas
- Reinforced past reports

- Firm gas may not be “firm”
- Load prediction models are limited
- We get what we expect from renewables
- Capacity energy ➡
- Retirements renewables ≠

- Retire 100 MW gas generator with solar/batteries
- 2400 MWh needed
- Assume average 8 hours of sunlight
- 100 MW during 8 hours (800 MWh)
- 100 MW storage during 16 hours (1600 MWh)
- 200 MW to charge storage during 8 hours (1600 MWh)
- Need 300 MW of solar and 1600MWh of storage
- Assumes no losses in conversion

Now what actions should be the focus?

- Cold weather standards
- Standard revisions for inverter-based resources
- Planning requirements that focus on energy sufficiency at all hours, not just “peak”
- Registering inverter based resources
- Outreach to states to coordinate efforts on distribution

- Facility Ratings Task Force – consistency
- Focus on risk and methodology
- Potential future FAC-008 modification

- December 15, 2022 FERC order
 - Is the applicability criteria appropriate?
 - Is the risk assessment adequate?
 - Should a minimum level of physical protection be established?
- Report filed April 14, 2023
 - Purpose of CIP-014 is to protect against “evil three” not load loss
 - Current applicability meets purpose
 - Additional clarity needed concerning risk assessment
 - Minimum level of physical protection for all substations not needed
- Technical conference August 10 in Atlanta

A stylized map of North America, including the United States, Canada, and Mexico. The map is rendered in shades of blue and grey. A prominent horizontal band of a darker blue color stretches across the middle of the map, serving as a background for the title text.

Questions and Answers

15 Minute Break!

**Annual HERO
Award**
**Nominate Someone
Today!**



MIDWEST
RELIABILITY
ORGANIZATION

www.mro.net/about/hero/



HERO

HIGHLY EFFECTIVE RELIABILITY ORGANIZATION





MIDWEST
RELIABILITY
ORGANIZATION

Compliance Monitoring and Enforcement Report (CMEP) Overview

Tasha Ward

Director of Enforcement and External Affairs

2023 MRO CMEP Hybrid Conference

July 26, 2023

Agenda

- **Purpose**
- **Overview**
- **Risk Assessment and Mitigation**
 - Compliance Severity Index (CSI)/Highest Risk Standards
 - Risk Determinations
- **Enforcement**
 - Entity Responsibility
 - Discovery Methods
 - Dispositions of Issues of Noncompliance

Purpose

Quarterly CMEP Summary Report

Midwest Reliability Organization

December 31, 2022

This document was prepared for the Midwest Reliability Organization (MRO) Board of Directors to provide a quarterly summary of areas addressing key issues, trends, and significant events in the MRO region related to its delegated authorities set forth in the Compliance Monitoring and Enforcement Program (CMEP).



Overview

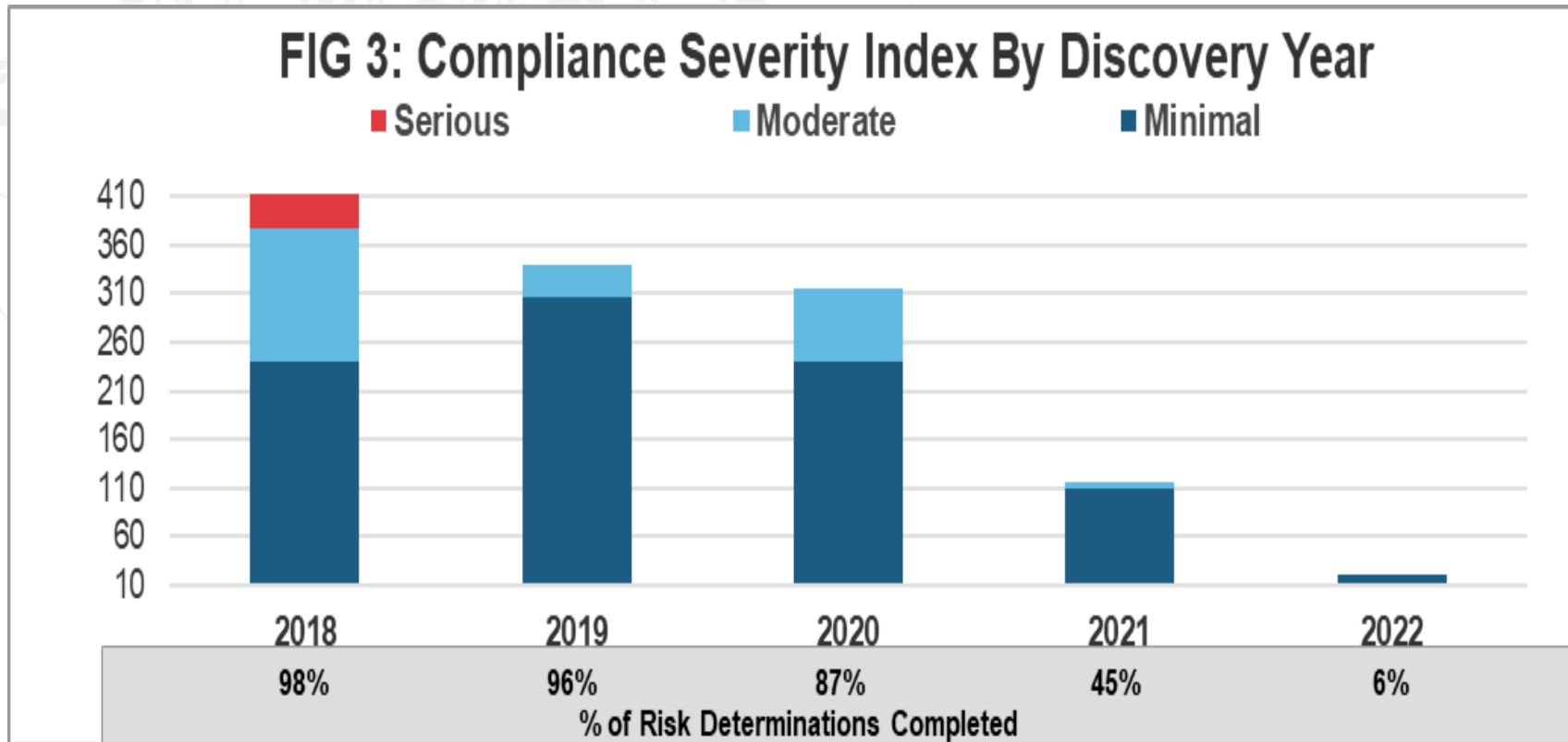
- **Compliance**
 - Compliance Oversight Plan
 - Compliance Audits
 - Self-Certifications
- **Risk Assessment and Mitigation**
 - Compliance Severity Index/Highest Risk Standards
 - Risk Determinations
- **Enforcement**
 - Disposition of Issues of Noncompliance
 - Age of Noncompliance



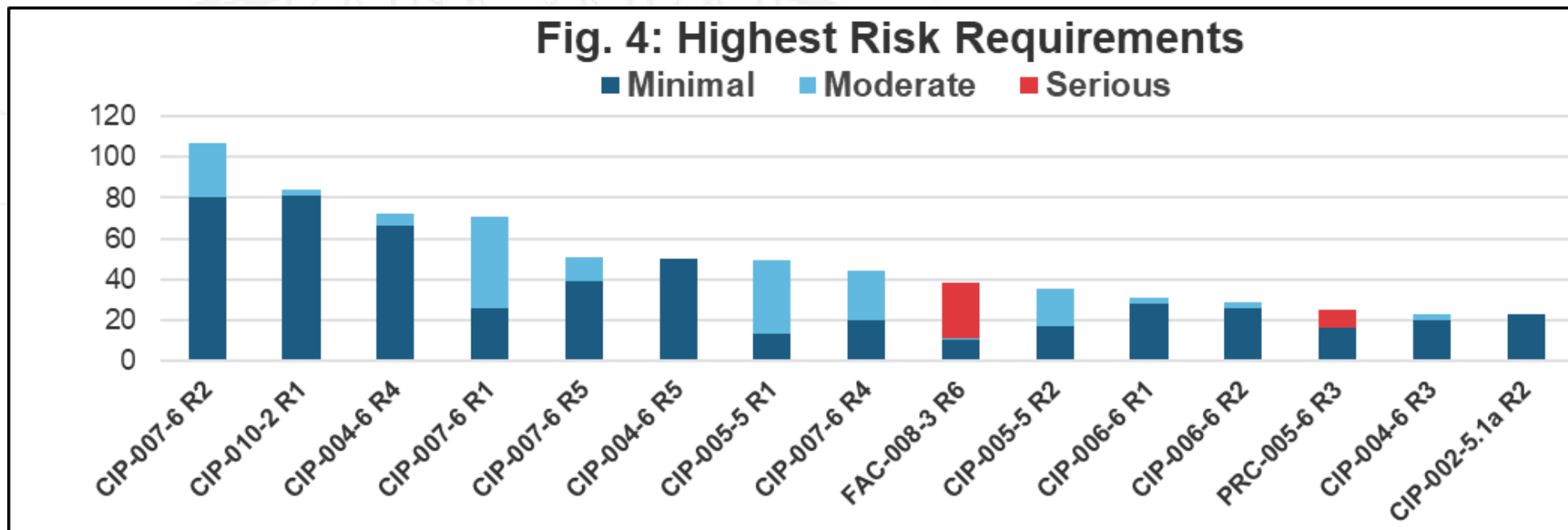
Compliance Severity Index

- **Calculated using a combination of the risk determination and discovery method**
- **Represents total risk that issues of noncompliance pose to the reliability and security of the bulk power system in MRO's region**

Compliance Severity Index

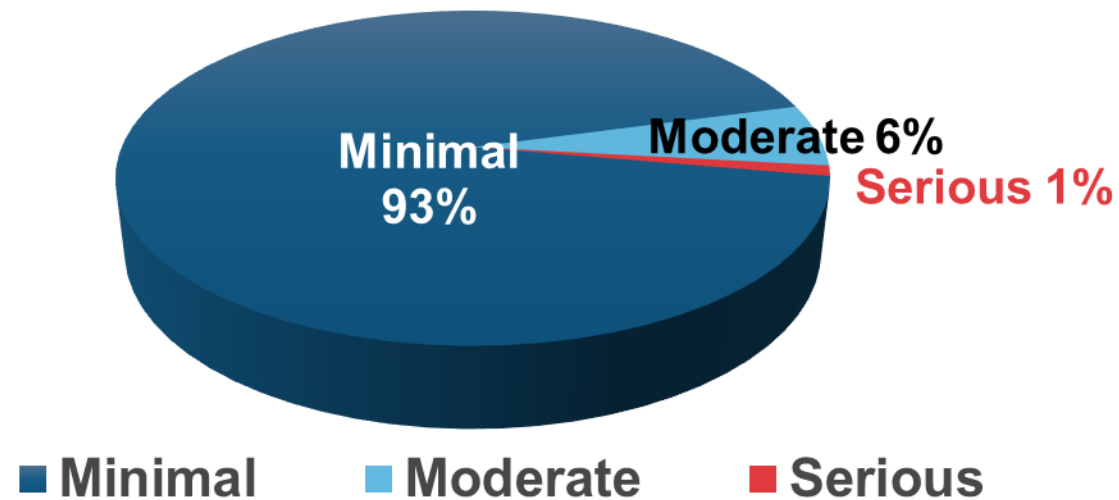


Highest Risk Requirements



Risk Determinations

**Fig. 5: Risk Determinations for
Instances of Noncompliance**
(January 1, 2017-December 31, 2022)



Noncompliance Statistics

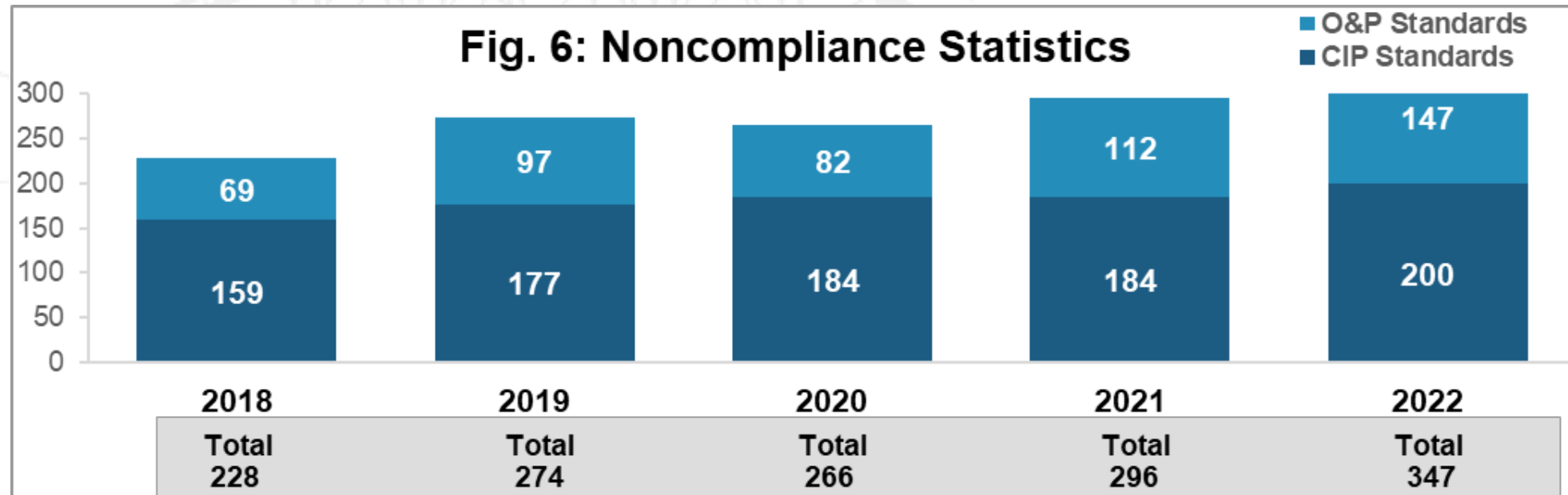


Figure 6 shows a breakdown of Critical Infrastructure Protection (CIP) vs. Non-CIP Possible Issues of Noncompliance

Self-Identified Noncompliance

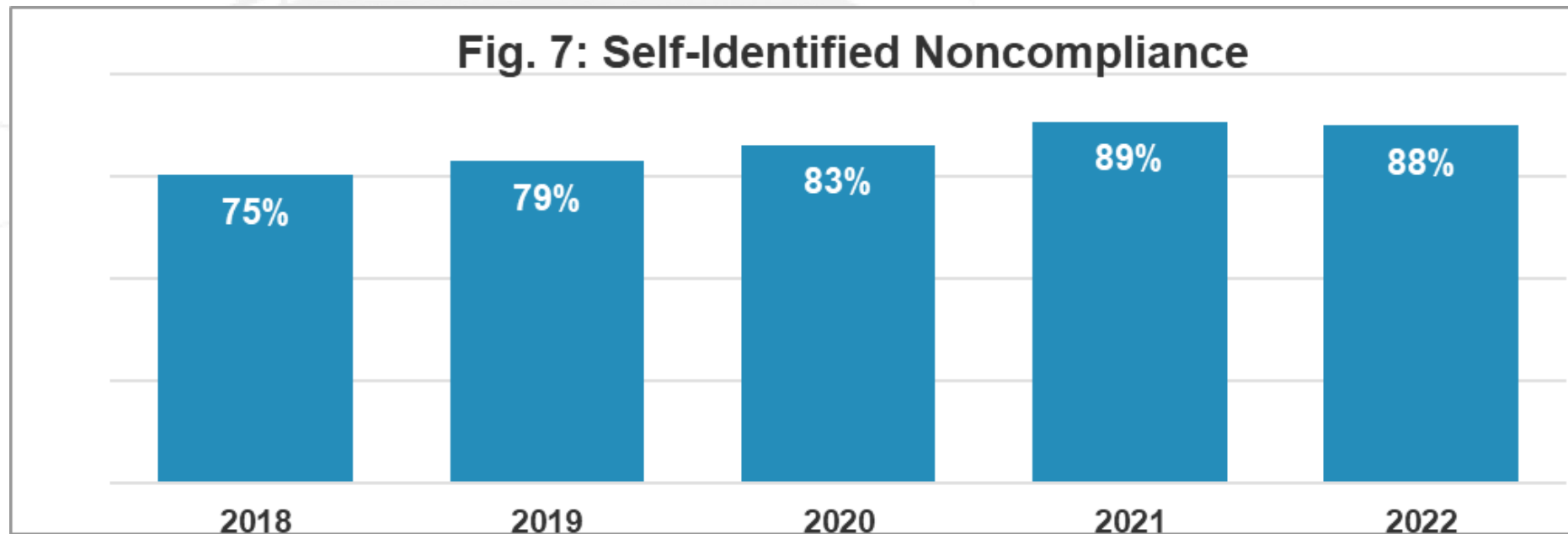


Figure 7 reflects issues of self-identified noncompliance that MRO processed from January 1, 2018, to December 31, 2022.

Registered Entity Acceptance

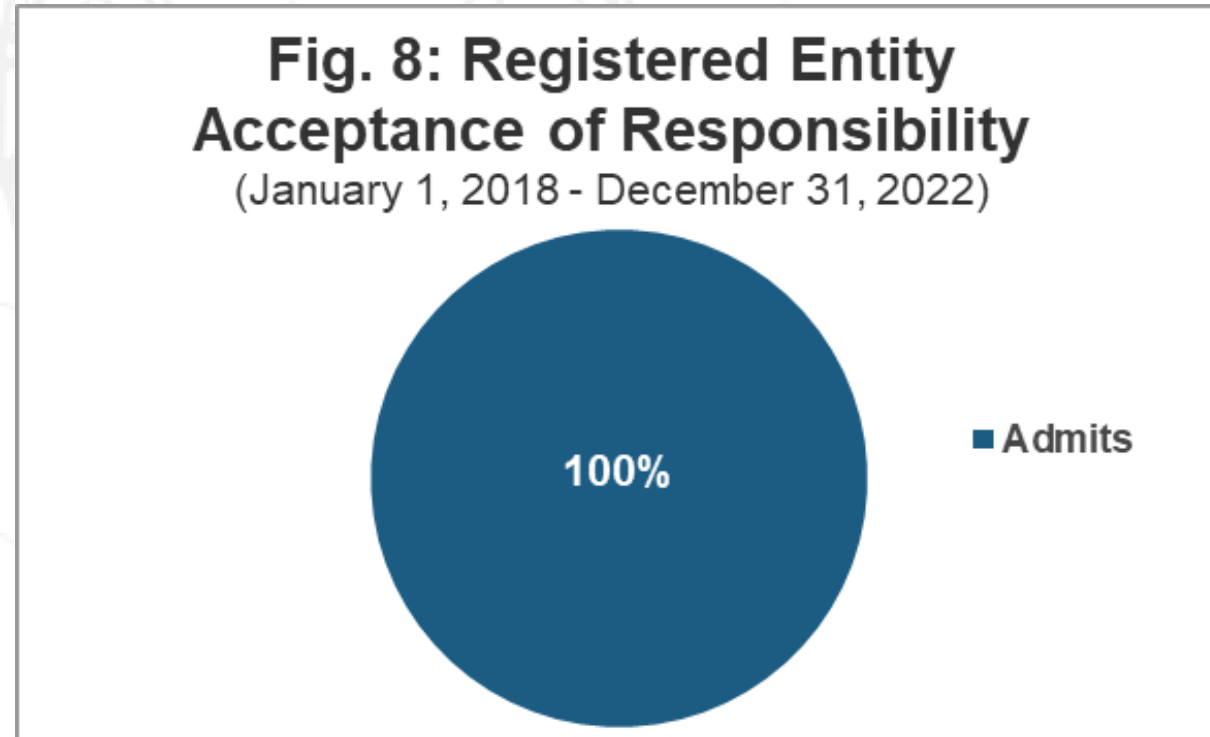


Figure 8 shows the percentage of time that registered entities have accepted responsibility for noncompliance submitted to NERC or other applicable Regulatory Authority from January 1, 2018 through December 31, 2022.

Discovery Method

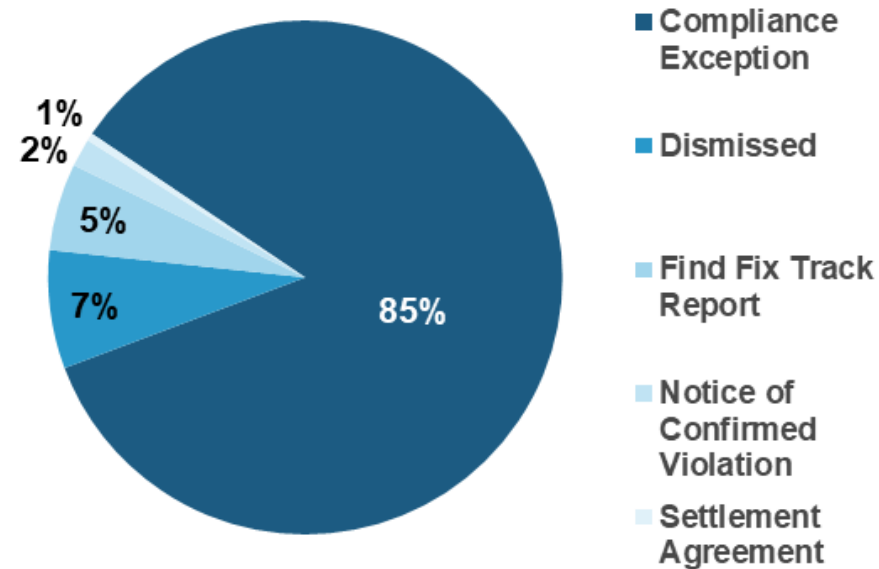
Figure 9: Discovery Method

Discovery Method Detail	2018	2019	2020	2021	2022	Sub Total	(-less) Dismissed	Total
Compliance Audit	33	47	40	18	18	156	19	137
Compliance Investigation	0	0	0	0	0	0	0	0
Data Submittal	0	0	0	0	0	0	0	0
Self-Certification	23	11	6	16	24	80	11	69
Self-Log	97	130	145	155	182	709	7	702
Self-Report	75	86	75	107	123	466	26	440
Spot Check	0	0	0	0	0	0	0	0
Totals	228	274	266	296	347	1411	63	1348

Disposition Method

Fig. 10: Processing Method Percentages

(January 1, 2018 - December 31, 2022)



Questions

- **Contact Information:**

Tasha Ward
Director of Enforcement and
External Affairs
tasha.ward@mro.net
651-256-5188

Janice Anderson
Enforcement Paralegal
janice.anderson@mro.net
651-855-1720

Bill Steiner
Director of Compliance
Monitoring
william.steiner@mro.net
651-256-5188





MIDWEST
RELIABILITY
ORGANIZATION

Demonstrating Positive Performance

Jess Syring, CIP Compliance Manager

2023 MRO CMEP Hybrid Conference

July 26, 2023

CLARITY

ASSURANCE

RESULTS

Agenda

- **Positive performance aspects**
 - Current definition/criteria
 - Proposed definition/criteria
- **What are the impacts of this designation?**
- **Examples of demonstrated positive performance**



Positive Performance Aspects

- **Current definition:**
 - Performance consideration is a data point or piece of information that Regional Entity's consider to understand an entity's performance to identify entity-specific risks
 - Definition taken from the NERC COP FAQ document posted on the website
- **Performance consideration is qualitative and dependent on known facts and circumstances**



Positive Performance Aspects

- **Criteria utilized**
 - Affiliates
 - Compliance History
 - Culture of Compliance
 - Events
 - Misoperations
 - Internal Controls



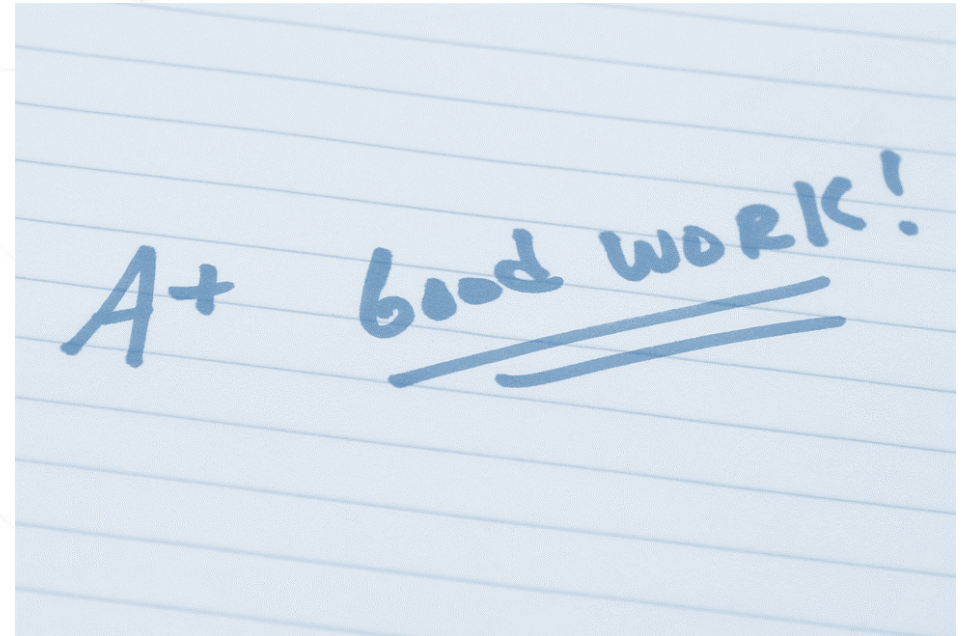
Positive Performance Aspects

- **Proposed future definition**
 - A Performance Consideration consists of available data points or pieces of information the Regional Entities consider to identify entity-specific performance risks (Inherent Risk is analyzed using the Risk Factors), which are quantitative and qualitative and dependent on other known facts and circumstances
- **This is currently being developed and is expected to be final prior to the end of 2023**



Positive Performance Aspects

- **Draft criteria**
 - Compliance History
 - Culture of Compliance
 - Events
 - Misoperations
 - Internal Controls
 - Generation
 - Transmission



Positive Performance Aspects

- **Compliance History**

- Analysis includes a review of a registered entity's past violations
 - Number
 - Severity of past violations
 - Review of repeat/common root causes compared to other entities of similar size and makeup
- Violations of Non-Compliance are found via Self-Reports and CMEP activity findings
- Align will be the data source for this analysis



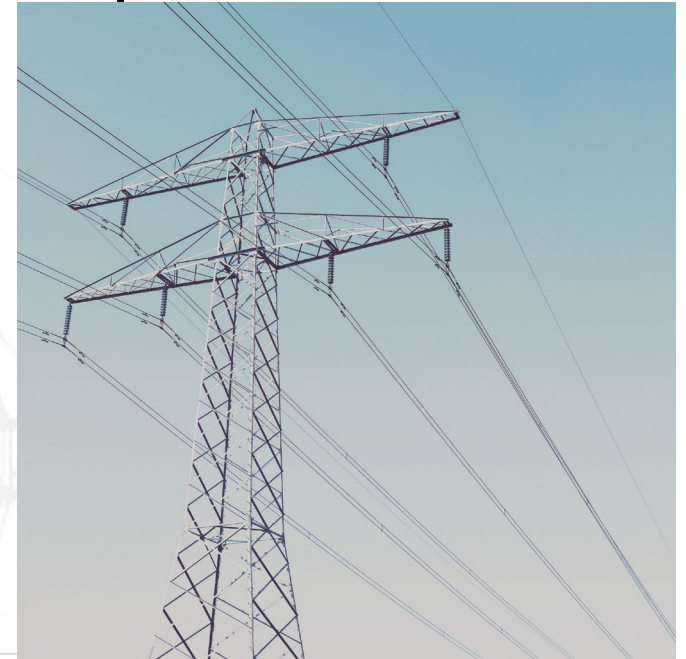
Positive Performance Aspects

- **Culture of Compliance**
 - Analysis includes a review of the organizational characteristics
 - Self-logging privileges
 - Timing of Self-Reports
 - Strong or weak evidence submittals
 - Feedback on entity culture of compliance via CMEP activities



Positive Performance Aspects

- **Events, Misoperations, Generation, and Transmission**
 - Analysis is completed by the Risk Analysis department



CLARITY

ASSURANCE

RESULTS

Positive Performance Aspects

- **Internal Controls**

- Analysis includes a review of internal controls as well
 - Results of testing and other internal control information identified during CMEP activities
- Still a lot of ERO discussion as to what this entails
 - Global could be focused on the overall performance criteria
 - Specific internal controls for standards would be shared and assist with selecting the risk categories, as well as supporting evidence for the operational effectiveness supporting the global internal control program



What are the Impacts of the Delegation?

- **Helps to determine the category within the Compliance Oversight Plan**

Category	Category Description	Target Monitoring Interval
1	Represents an entity that has higher inherent risk without demonstrated positive performance considerations.	Every 1-3 years
2	Represents an entity that has higher inherent risk with demonstrated positive performance considerations.	Every 2-4 years
3	Represents an entity that has moderate inherent risk without demonstrated positive performance considerations.	Every 3-5 years
4	Represents an entity that has moderate inherent risk with demonstrated positive performance considerations.	Every 4–6 years
5	Represents an entity that has lower inherent risk without demonstrated positive performance considerations.	Every 5-7 years
6	Represents an entity that has lower inherent risk with demonstrated positive performance considerations.	Every 6+ years



Examples

Positive

- **Transparency of sharing of internal controls**
- **Included in optional activities with detailed submittals**
- **Limited amount of RFIs and SME interviews**

Negative

- **Multiple severe violations with repeat causes**
- **Unwillingness to share information beyond compliance with the standards**





QUESTIONS?



Break for Lunch!

**Annual HERO
Award**
**Nominate Someone
Today!**



MIDWEST
RELIABILITY
ORGANIZATION

www.mro.net/about/hero/



HERO

HIGHLY EFFECTIVE RELIABILITY ORGANIZATION





Order No. 893

Incentives for Advanced Cybersecurity Investment

MRO's CMEP Advisory Council

July 26, 2023

David DeFalaise, Office of Electric Reliability
Energy Infrastructure & Cybersecurity Advisor



All information contained in this presentation and any statement from an individual presenter are the opinions and views of that presenter, unless specifically stated, and not necessarily that of:

- The United States Government;
- The Federal Energy Regulatory Commission;
- Individual Commissioners; or
- Other members of the Commission staff.



Order No. 893 Timeline

Milestone	Date
Infrastructure Investment and Jobs Act (IIJA) Signed Into Law	November 15, 2021
NOPR Issued by FERC	September 20, 2022
Final Rule Issued by FERC	April 21, 2023
The Rule is Effective	July 3, 2023
Order on Rehearing or Clarification (one request filed from NRECA)	TBD



Infrastructure Investment and Jobs Act of 2021 (IIJA)

Section 40123 of the IIJA added section 219A to the Federal Power Act that directed FERC to:

- **Establish** incentive-based rate treatments for transmission and wholesale sale of electric energy in interstate commerce;
- **To** encourage investments in:
 - Advanced Cybersecurity Technology; and
 - Participation in Cybersecurity Threat Information Sharing Programs.



Advanced Cybersecurity Technology

18 CFR § 35.48(b)

- Technology, operational capability, or service, including computer hardware, software, or a related asset;
- Enhances the security posture of public utilities;
- To protect against, detect, respond to, or recover from a “cybersecurity threat.”

6 USC § 1501(5)



Incentive-based Rate Treatment for Cybersecurity Investment

18 CFR § 35.48(c)

- **Voluntarily**
 - makes an investment in Advanced Cybersecurity Technology; or
 - participates in a cybersecurity threat information sharing program
- **Demonstrates** that the resulting rate is
 - just and reasonable; and 16 USC § 824d(a)
 - not unduly discriminatory or preferential 16 USC § 824d(b)
- **Available to**
 - public and non-public utilities;
 - that have or will have a cost-based rate on file with FERC



Eligibility Criteria

18 CFR § 35.48(d)

- **Materially improves** cybersecurity through either Advanced Cybersecurity Technology or participation in a cybersecurity threat information sharing program;
- **Not already mandated by**
 - FERC-approved Reliability Standards;
 - Local, State, or Federal law, decision, or directive;
 - Otherwise legally mandated, such as:
 - Merger condition;
 - Consent decree from Federal or State agency, or
 - Settlement agreement.



Demonstrating Satisfaction of the Eligibility Criteria

18 CFR § 35.48(e)

1. Pre-Qualified Cybersecurity Investment (PQ List)
 - Rebuttable Presumption
 - PQ List maintained on FERC's website
2. Case by Case
 - No rebuttable presumption
3. Early Compliance with an approved but not yet effective cybersecurity-related CIP Reliability Standards
 - Terminates when Reliability Standard becomes effective



PQ List

18 CFR § 35.48(e)(1)

- **Initial PQ List Technology:** Order No. 893 P 54
 1. Cybersecurity Risk Information Sharing Program (CRISP); and
 2. Internal Network Security Monitoring
- **Posted on FERC's public website** Order No. 893 P 69
 - Actual location is coming soon...
- **Updated by** Order No. 893 P 69
 - Notice and comment period; or
 - Rulemaking



Materially Improve

PQ List

Order No. 893 P 40

1. NIST SP 800–53;
2. NIST Cybersecurity Framework;
3. Recommendation from relevant Federal authority;
4. Participation in relevant cybersecurity threat information sharing program; **or**
5. Achieving highest MIL level of a C2M2 Domain.

Case by Case

Order No. 893 P 109

1. NIST CSF & SP 800–53; **and**
2. Recommendation from relevant Federal authority.



Incentive Structure

18 CFR § 35.48(f)

- Incentive-Based Rate Treatment = Deferral of Expenses as a Regulatory Asset
- For ratemaking, allows utilities to include eligible expenses in rate base and earn a rate of return on those expenses.
- Incentive lasts for up to five years, with amortization of costs being up to five years.



Incentive Duration

18 CFR § 35.48(g)

- Regulatory Asset (Advanced Cybersecurity Technology)
 - **Amortized** over a period of up to five years at applicant's choice;
 - **Limited** to first five years following Commission approval;
 - **Limited** to expenses starting no more than three months prior to filing;
 - **Terminated** when the cybersecurity becomes mandatory.
- Cybersecurity threat information sharing program
 - **Not Limited** to any duration, as long as participation is voluntary;
 - **Amortized** each year expenses over the next five years.



Incentive Application

18 CFR § 35.48(h)

1. **Filing** pursuant to section 205 of the Federal Power Act, or
2. **Petition** for a declaratory order that precedes the 205 filing.

Requests:

- Part of a general rate request; or
- Single-issue basis.



Reporting Requirements

18 CFR § 35.48(i)

- **Annual** informational filing due June 1
 - **For** incentive-based rate treatment approved at least 60 days prior to June 1 of that year
 - **Detailing** specific cybersecurity investments with corresponding FERC account used
 - **Describing** the deferred expenses to differentiate cybersecurity improvement from ongoing maintenance



Protection of Cybersecurity Information

18 CFR § 35.48(j)

- **Transmitted** as Critical Energy/Electric Infrastructure Information (CEII) 16 USC § 824o-1
- **Applies to:** 18 CFR § 388.113(d)(1)(i)–(ii)
 - Incentive Application; **and/or**
 - Annual Reporting



FERC's Website

- Incentives
<https://www.ferc.gov/incentives>
- Transmission Incentives
<https://www.ferc.gov/transmission-incentives>
- Cybersecurity Incentives
<https://www.ferc.gov/cybersecurity-incentives>
- Pre-qualified List (PQ List)
<https://www.ferc.gov/pre-qualified-list-pq-list>



Questions & Answers

Legal Questions

Alan Rukin

Attorney-Advisor

Office of General Counsel

Rate Questions

Adam Pollock

Energy Industry Analyst

Office of Energy Market Regulation

Cybersecurity Questions

Justin Storms

IT Specialist (Cybersecurity)

Office of Energy Infrastructure Security





MIDWEST
RELIABILITY
ORGANIZATION

BCSI and the Cloud NERC Project 2019-02 CIP-004-7 and CIP-011-3 Implementation

Josh Powers

Southwest Power Pool (SPP)

Compliance Supervisor, SPP; 2019-02 SDT Vice Chair

2023 MRO CMEP Hybrid Conference

July 26, 2023

Agenda

- **Purpose of Project 2019-02**
- **Important Concepts**
 - Obtain and Use
 - Provisioned Access
- **Backwards Compatibility**
- **Summary of Changes**
- **CIP-011-3 and CIP-004-7**
- **Important Dates**
- **Implementation**



Purpose of Project 2019-02

- Clarify CIP requirements related to both managing access and securing Bulk Electric System (BES) Cyber System Information (BCSI)
- Enhance Bulk Electric System (BES) reliability by creating increased choice, greater flexibility, higher availability, and reduced-cost options for entities to manage BCSI
- Clarify the protections expected when utilizing third-party solutions (e.g., cloud services)
- Proposed revisions to Reliability Standards CIP-004-6 and CIP-011-2
- NOTE: Scope does NOT include BES Operations in the cloud



Important Concepts

- **Access:**
 - the ability to obtain and use
- **Provisioned access:**
 - the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys)



Obtain

On-premise

- Your vehicle
- Locked
- In garage
- Your house

Off-premise

- Parked on street
- Parking garage
- Tow truck
- Locked/secure



Use

- **Keys to your car**
 - Separation of duties (locks and keys)
 - Custodial control (keys in your hands or your spouse's possession)
 - Even if you do not possess the car, others cannot use the car



Provisioned Access

- **Main point = access by authorized individuals to BCSI within your entity's control**
 - For an individual, not a system
 - Authorized
 - Based on need (determined by entity)
 - Periodically reviewed
 - Ability removed for individual connected to termination action
- **Other forms of access need to be addressed in your entity's information protection program (e.g., unauthorized access, authorized system access)**



Backwards Compatibility

- **Addresses hindrance to using cloud**
- **Less prescriptive language enables other methods (e.g., encryption) for access management**
- **Entities can still use designated storage locations**
- **Access to BCSi residing on BCS, Electronic Access Control and Monitoring System (EACMS), and Physical Access Control Systems (PACS) addressed through R4 access management program; do not need to repeat provisioning access to BCSi via R6**



Summary of Changes

CIP-004-7

- BCSI access management consolidated into one requirement (R6)
- Changed to “provisioned access to BCSI”
- Included concept of “obtain and use” from CMEP practice guide
- Clarified requirements for physical and electronic

CIP-011-3

- Focus on BCSI that pertains to the Applicable Systems
- Mitigating the risk of compromising BCSI confidentiality
- R1 simplified to provide greater clarity and flexibility in implementing information protection



CIP-011-3, R1

- Each Responsible Entity shall implement one or more documented information protection program(s) for BES Cyber System Information (BCSI) pertaining to “Applicable Systems” identified in *CIP-011-3 Table R1 – Information Protection Program* that collectively includes each of the applicable requirement parts in *CIP-011-3 Table R1 – Information Protection Program*



CIP-011-3, R1, Part 1.1

CIP-011-2

- Method(s) to identify information that meets the definition of BES Cyber System Information

CIP-011-3

- Method(s) to identify BCSI



CIP-011-3, R1, Part 1.2

CIP-011-2

- Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use

CIP-011-3

- Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality



CIP-004-7, R6

- Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSi pertaining to the “Applicable Systems” identified in CIP-004-7 Table R6 – Access Management for BES Cyber System Information that collectively include each of the applicable requirement parts in *CIP-004-7 Table R6 – Access Management for BES Cyber System Information*. To be considered access to BCSi in the context of this requirement, an individual has both the ability to obtain and use BCSi. Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSi (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys).



CIP-004-7, R6, Part 6.1

CIP-004-6 (R4, Part 4.1)

- Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:
- 4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.

CIP-004-7 (R6, Part 6.1)

- Prior to provisioning, authorize (unless already authorized according to Part 4.1.) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:
- 6.1.1. Provisioned electronic access to electronic BCSI; and
- 6.1.2. Provisioned physical access to physical BCSI.



CIP-004-7, R6, Part 6.2

CIP-004-6 (R4, Part 4.4)

- 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.

CIP-004-7 (R6, Part 6.2)

- Verify at least once every 15 calendar months that all individuals with provisioned access to BCSI:
 - 6.2.1. have an authorization record; and
 - 6.2.2. still need the provisioned access to perform their current work functions, as determined by the Responsible Entity.



CIP-004-7, R6, Part 6.3

CIP-004-6 (R5, Part 5.3)

- 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.

CIP-004-7 (R6, Part 6.3)

- For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action.



Important Dates

NERC and FERC Approvals

- **NERC BOT Adoption: 8/12/2021**
- **NERC Filing to FERC: 9/15/2021**
- **FERC Approval: 12/7/2021**
 - Docket No. RD21-6-000
 - 20211207-3062

Implementation

- **Effective Date: 1/1/2024**
- **Entities may elect to comply with CIP-004-7 and CIP-011-3 prior to 1/1/2024 (early adoption)**
 - Notify applicable Regional Entities of the date of compliance with the CIP-004-7 and CIP-011-3 Reliability Standards
 - Notify at least 90 days before early implementation date



Implementation

- **Controls, controls, controls**
 - Prevent CSP staff from the ability to use BCSI
 - Electronic technical methods to protect electronic BCSI
 - Physical technical methods to protect physical BCSI
 - Administrative method(s) to protect BCSI
 - Think about endpoints from your entity to the CSP and what controls are needed to comprehensively protect BCSI
 - CSP relationships change; access management and information protection programs need to incorporate CSP on-boarding/off-boarding



Implementation (Cont.)

- **CSP risk assessments are a good thing (and not required)**
- **Some items to consider for mitigating risk:**
 - Data sovereignty and backups – where will your BCSI be stored?
 - Fault tolerance – what happens if something fails or is interrupted?
 - Multi-factor authentication – defense in depth
 - SIEM integration – audit logging availability
 - Vulnerability management – frequency and access to results
 - Legal limitations on what mitigation can be applied



Primary NERC References/Links

- [CIP-004-7](#)
- [CIP-011-3](#)
- [Project 2019-02 Implementation Plan](#)
- [CIP-004 Technical Rationale](#)
- [CIP-011 Technical Rationale](#)
- [ERO CMEP Practice Guide: BES Cyber System Information](#)



Additional References/Links

- [Early Adoption of Revised Reliability Standards \(MRO article\)](#)
- [BCSI Revisions \(RF article\)](#)
- [NIST Special Publication 800-209](#)
- [Security guideline for cloud solutions and encrypting BCSI](#)
- [Security guideline for risks related to CSPs](#)





MIDWEST
RELIABILITY
ORGANIZATION

Virtualization NERC Project 2016-02 Modifications to CIP Standards CMEP Workshop 2023

Sharon Koller

Lead Compliance Strategist & CIP Sr. Mgr., ATC

2023 MRO CMEP Hybrid Conference

July 26, 2023

CLARITY

ASSURANCE

RESULTS

Agenda

- **Purpose of Project 2016-02 | History and Focus of Presentation**
- **Overview of SDT Objectives & Important Concepts**
 - Enable CIP Standards for Secure Virtualization methods
 - Remove Encumbrances / Disincentives to Virtualize
 - Objective Requirements vs Prescriptive Lists
 - Reduce Administrative Overhead
 - Maintain Backwards Compatibility
- **Recap of Draft 4 Ballot Results**
- **Key Commenter Themes and SDT Considerations**
- **Draft 5 Status and Posting Schedule**



History & Focus of Today's Update

2016-02 SDT formed to address multiple items:

- **CIP V5 Transition Advisory Group (V5TAG)**
- FERC Order 822
- CIP Exceptional Circumstances

V5TAG Issues included

- Cyber Asset and BES Cyber Asset Definitions
- Network and externally accessible devices
- TO Control Centers performing TOP obligations
- **Virtualization**



Overview SDT Objectives

Entities have been virtualizing systems for decades now and have found means to implement in a compliant manner.

Others may have an appetite to virtualize, but certain administrative burdens, or lack of clarity within the current CIP Standards serve as a disincentive or are perceived as compliance risk.

A key objective of the SDT is not just to enable the CIP Standards for virtualization to open the toolbox for this option, but rather the intention to remove encumbrances, while maintaining security and backwards compatibility.



Recap of Draft 4 Ballot Results

Draft 4 (10/10/22)	Draft 5 Scope
CIP-002-7 ✓	CIP-005-8
CIP-003-Y ✓	
CIP-004-8 ✓	
CIP-005-8 ✗	CIP-005-8
CIP-006-7 ✓	CIP-007-7
CIP-007-7 ✓	
CIP-008-7 ✓	
CIP-009-7 ✓	CIP-010-5
CIP-010-5 ✗	
CIP-011-4 ✓	
CIP-013-3 ✓	

While draft 4 of CIP-007-7 passed, it was by a narrow margin, the SDT acknowledges improvement opportunities from industry comments, and will be addressing concerns in a 5th draft.



Key Commenter Themes

CIP-005-8

- **Applicable Systems and Shared Cyber Infrastructure (SCI)**
- **Consideration of Electronic Access Point (EAP) vs Electronic Access Point (ESP)**
- **Use of “per system capability”**
- **Management Interface scope/requirements**
 - **Protecting ESP configurations**
 - **Protecting SCI configurations**
- **“Internet Protocol” vs “routable protocol”**
- **Interactive Remote Access (IRA)**
 - **Use of the word “authorized”**
 - **Intent vs capability (humans vs. systems)**
 - **Routable to serial considerations/use cases**
- **Intermediate Systems**
 - **Protection of data vs. protection of link**
 - **“To” vs “Through” | “Inside” vs “Outside”**
 - **Sharing of “CPU and memory resources”**



Key Commenter Themes

CIP-007-7

- **CIP-007 vs CIP-005 concepts**
 - “Needed routable protocol network accessibility” (CIP-007 Cyber System level)
 - Needed routable protocol communications” (CIP-005 ESP level)
- **SCI applicability and scoping**
 - “CPU and memory resources”
 - EACMS & PACS backwards compatibility
 - PCA implications
- **Concept considerations and scoping**
 - “Ports and Services” vs “System Hardening”
 - “Prevent” vs “Mitigate”
- **Consistency/clarity in phrasing – mix of**
 - “security patching” vs “cyber security patching”
 - “logs/logging” vs “security logs/logging”



Key Commenter Themes

CIP-010-5

- **R1 Change Control**
 - Prescriptive baselines vs. objective concepts
 - Shift from documentation burden to security value
(*Authorize change instead of update docs after change*)
 - Define scope / floor
 - In scope: Use change control to authorize modifications affecting system behaviors
(*Security settings a system admin configures*)
 - Out-of-scope: Do not need change control to change password as expected.
(*What a user does, or how the system operates in reaction to what the system admin configures*)
 - Order of operations | implement vs. verify
 - Non-virtual: implement, verify
 - Virtual: verify (remediation VLAN), promote
 - Assure no unintended gaps
 - Assure backward compatibility with baseline concept



Key Commenter Themes

CIP-010-5 (continued)

- **R1/R2 monitoring control alignment/scope**
 - Not intended to be a mini-audit of CIP-005/007
 - Performed analysis of CIP-005/007 controls; mapped to baseline attributes
 - Re-focused R2 monitoring on CIP-007 controls:
 - Removes unintended expansion in scope
 - Restores backwards compatibility with baselining concepts
- **R3 Vulnerability Assessment**
 - Clarity on “like replacements” exclusion
 - Revised language to exclude replacements or additions of Applicable Systems with “previously assessed configurations”
- **R4 TCA**
 - Considered last known good state to address commenter concerns regarding, “*Controls that maintain the state of the operating system and software such that it is in a known state prior to execution;*”



Key Commenter Themes

Definitions

- **Cyber Assets – use of the term containers**
- **EACMS – Scope/hall of mirrors concerns**
 - If SCI must have an EACMS, but can also be an EACMS – where does the EACMS end?
 - Intermediate Systems as EACMS and non-routable protocol converter as an EACMS
- **EAP/ESP/ERC/IRA**
 - Relation between them
 - “To” vs. “through”; “inside” vs. “outside”
 - System to system vs. human interaction
 - Routable to serial conversion IRA
- **Management Interface – what it configures**
- **PCA – consideration of exclusions**
- **Shared Cyber Infrastructure (SCI) and where it should (or should not) exist in other definitions**
- **TCA – connected “to” vs. “on”; VCA on TCA**



Draft 5 Posting Status and Approach

Goal to post for comment and ballot in August 2023

Draft 5 Posting to include:

- CIP-005-8
- CIP-007-7 *(Even though draft 4 passed, it was by a small enough margin that the SDT is proposing modifications to address industry concerns.)*
- CIP-010-5
- New / Revised Definitions

Technical Rationale is being updated and expected to post alongside these proposed revisions.

Final Balloting will occur for the suite of CIP Standards CIP-002 – CIP-011, CIP-013, and New/Revised Definitions once industry approval is obtained for all.



Joint Q&A for SDT Updates

- **2019-02 BCSI and the Cloud**
 - Josh Powers
 - Compliance Supervisor, SPP; 2019-02 SDT Vice Chair
- **2016-02 Virtualization**
 - Sharon Koller
 - Lead Compliance Strategist & CIP Sr. Mgr., ATC; 2016-02 SDT Member



15 Minute Break!

**Annual HERO
Award**
**Nominate Someone
Today!**



MIDWEST
RELIABILITY
ORGANIZATION

www.mro.net/about/hero/



HERO

HIGHLY EFFECTIVE RELIABILITY ORGANIZATION





MIDWEST
RELIABILITY
ORGANIZATION

CIP-014-3 R1

Assessment Observations and Common Practices

Sam Zewdie
2023 MRO CMEP Hybrid Conference
July 26, 2023

Reliability Standard CIP-014-3

- CIP-014-3 became effective on June 16, 2022
 - V3 removed the provision that evidence be retained at the transmission owner's or transmission operator's facility
- CIP-014-3 evidence can be placed in the **Secure Evidence Locker**
 - CIP Evidence Request (ERT) Tool – Version 7

CMEP Practice Guide

- ERO Enterprise CMEP Practice Guide: CIP-014-3 R1

- The ERO Enterprise identified a need to for a common approach to auditing CIP-014-3 R1
- Initially approved November 2021 and was updated September 2022
- Posted for transparency on the NERC website

CIP-014-3 Audits

- **Conducted by CIP and O&P teams**
 - **Purpose:** To identify and protect substations, and associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in **instability, uncontrolled separation, or Cascading** within an interconnection

Applicability

- **Determine entity involvement in coordinating with the larger area (TP/PC/RC)**
 - Joint ownership should be considered
 - Consider normally open lines
 - Applicability mirrors bright line criteria for “medium impact” Transmission Facilities under Attachment 1 or Reliability Standard CIP-002-5.1a

Defined Terminology

- **Uncontrolled separation - not NERC defined**

Uncontrolled separation: the unintended islanding of a portion of an electric system that includes generation, load, or a combination of the two. Unintended refers to the unplanned removal of a portion of the electric system due to operation of protection or control systems.

Defined Terminology

- **Instability** - not NERC defined

But **Stability** is: The ability of an electric system to maintain a state of equilibrium during normal and abnormal conditions or disturbances.

Defined Terminology

- **Cascading - NERC defined term**

Cascading: The uncontrolled successive loss of system elements triggered by an incident at any location. Cascading results in widespread electric service interruption that cannot be restrained from sequentially spreading beyond an area predetermined by studies.

R1 Audit Considerations

- **Is the risk assessment effective at identifying critical substations?**
- **Does the risk assessment have reasonable criteria, study methodology, and assumptions?**
- **What about the case(s) used?**
- **TO relying on the results of past studies?**

Study Must Haves

- **Dynamic study in addition to steady state analysis**
 - How robust are the criteria developed? Study decisions made by an unaffiliated party? Entity is actually involved in study decisions or just “present”?
- **Criteria for steady state/dynamic**
 - Stability assessment
 - Uncontrolled separation assessment
 - Cascading analysis

Study Must Haves

- **Is study set up in a way to be able to test the criteria developed?**
- **Loss of entire substation (smoking crater)**
 - Are they removed simultaneously?
- **Delayed remote clearing**

Study Must Haves

- If using a generic fault clearing time, it has to be more conservative than the actual fault clearing time
- Monitor a wider area to include the impact of the area
- Identify and resolve problems in the base case models

Common Practices to Consider

- **Transmission Owners without critical substations include a five-year out model**
- **Have cases that show different stress conditions**
- **Consider the impact of future projects from neighbors' footprints**
- **Consider impact of undervoltage load shedding (UVLS), underfrequency load shedding (UFLS), and Remedial Action Scheme (RAS)**

Common Practices to Consider

- **Criteria need to be specific, not abstract**
- **Monitor voltage and frequency at generator buses**
- **Consider substations that are physically very close regardless of ownership**
 - An easy line of sight, access from common public roadway, and proximity that a single event can impact both substations

Common Practices to Consider

- **Document assumptions used**
 - For effective and consistent implementation
- **Document consequential and nonconsequential load and generation loss**
- **Incorporate the load and generation impact from the dynamic simulation as a starting point for the steady state study**
- **Run the simulation for no less than 10 seconds**

NERC Report on Physical Security

- No recommended changes to applicability criteria
- NERC will hold a technical conference
- Add specificity to criteria expectations
- NERC plans to initiate a Reliability Standards development project
- No recommended minimum physical security

Read the full [NERC Report on Physical Security](#)

Questions?

Send questions to: Heros@mro.net





MIDWEST
RELIABILITY
ORGANIZATION

Streamlining the Standards Development Process

Amy Casuscelli

Manager of Reliability Assurance and Risk Mitigation, Xcel Energy

Chair of the NERC Standards Committee.

2023 MRO CMEP Hybrid Conference

July 26, 2023

CLARITY

ASSURANCE

RESULTS

Standards Process Improvements

- **Case for Change**
 - Workload
 - Need for increased agility
 - Opportunity for efficiencies
- **Standards Process Stakeholder Engagement Group (SPSEG)**



SPSEG Recommendations

- **Rules of Procedure**
- **Standing Committees**
- **Standard Processes Manual (SPM)**



SPM Changes

- **Supports removal of ANSI Accreditation Requirement**
 - Still preserves basic tenets of open, transparent and fair process
- **Clarifies certain roles of Standards Committee**
- **Final Ballot/Conclusion of Standards Action**



Success Story

- **SPM Ballot Results**
 - Initial: 38% approval
 - Final: 97% approval
- **Efficiency Gains**
- **Compromise via consensus**





Questions?

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Project 2021-07: Extreme Cold Weather Standard Drafting Team Update

Brad Pabian
July 26, 2023

RELIABILITY | RESILIENCE | SECURITY



- 2021-07 proposal for EOP-012-2 includes the following Key Recommendations from the Joint Inquiry Report:
 - 1a – GO identification of cold-weather-critical components and systems
 - 1b – GO identification and implementation of freeze protection measures on each of the elements identified per 1a
 - 1c – GO requirement to account for the effects of precipitation and wind
- Key Recommendations 1d, 1e, 1f, and 1j were included in Phase 1 of SDT
- Key Recommendations 1g, 1h, and 1i are included in revisions to EOP-011 and TOP-002
 - SDT continues work on those standards for future ballot

EOP-011

- Revision 2 currently effective, includes recently completed cold weather generation requirements, and transmission emergency operation requirements
- Revision 3 is industry and FERC approved, but implementation suspended pending EOP-012 since generation portion is moved
- Revision 4 was proposed to include Phase 2 recommendations. Industry ballot this spring was approximately 50-50, did not pass.

EOP-012

- Revision 1 currently effective, although FERC directed several changes with approval including standard applicability, timeframe for corrective actions, shortening of the implementation time for the standard, and clarification exceptions for units not in freezing conditions.
- Revision 2 proposed to include Phase 2 recommendations and FERC directed changes. Ballot window through July 20.

TOP-002

- Revision 4 currently effective
- Revision 5 was proposed to include Transmission and Balancing Authority Key Recommendations from SAR. Industry ballot this spring was approximately 50-50, did not pass

- Phase 2 includes the following directives from the FERC order to be included in EOP-012:
 - Applicability: Ensure the applicability section captures all BES generation resources needed for reliable operation and excludes only those generation resources not relied upon during freezing conditions.
 - Generator Constraints to Implementing Winterization Requirements: develop modifications related to generator-defined declarations of technical, commercial, or operational constraints that preclude a generator owner from implementing the appropriate freeze protection measures. Specifically, include auditable criteria on permissible constraints and to identify the appropriate entity that would receive the generator owners' constraint declarations.

- Phase 2 includes the following directives from the FERC order to be included in EOP-012:
 - Generator Capability Requirements: modifications to ensure that generators that are technically incapable of operating for 12 continuous hours (e.g., solar facilities during winter months with less than 12 hours of sunlight) are not excluded from complying with the standard. Also, directed modifications to the one-hour continuous operations requirement to better align with the stated purpose of the standard.
 - Corrective Action Plan deadlines: include a deadline or maximum period for the completion of corrective action plan measures for any requirement requiring the development of a corrective action plan to address capability or cold weather performance issues.
 - Implementation Plan: Require a shorter implementation period than five years after approval.

- SDT proposal to meet FERC directive for Applicability
 - Functional Entities: Generator Owner and Generator Operator (no change from EOP-012-1)
 - Clarification of Facilities: “Generating Unit” refers to
 - a BES resource identified in the BES definition, Inclusion I2 and I4
 - I2: Generating resource(s) including the generator terminals through the high-side of the step-up transformer(s) connected at a voltage of 100 kV or above with: a) Gross individual nameplate rating greater than 20 MVA, or b) Gross plant/facility aggregate nameplate rating greater than 75 MVA
 - I4: Dispersed power producing resources that aggregate to a total capacity greater than 75 MVA (gross nameplate rating), and that are connected through a system designed primarily for delivering such capacity to a common point of connection at a voltage of 100 kV or above
 - Blackstart Resource identified in the BES definition, Inclusion I3
 - Exclusions not prescribed in Applicability section
 - Any exemption moved to individual standard requirements in EOP-012-2

To better clarify the intent of the standard, the SDT created a proposed new NERC Glossary term, Generator Cold Weather Constraint(s) that contains three subcategories

- **Generator Cold Weather Constraint(s)** – A limitation that would prohibit a Generator Owner from implementing freeze protection measures on one or more Generator Cold Weather Components. A constraint must fall under one of the following areas:
 - Technical Constraints
 - Commercial Constraints
 - Operational Constraints

- EOP-012 revised to include maximum times for CAP execution
- CAPs may be required by R1, R2, R3, or R6 to provide new or corrected freeze protection measures
- NERC definition requires CAP to have a timetable for execution.
 - Actions that address existing equipment or freeze protection measures must be completed within 24 months of development of the CAP.
 - Actions that require new equipment or freeze protection measures must be completed within 48 months of development of the CAP.
- Generator Owners may declare a Generator Cold Weather Constraint (see definition) if unable to implement actions in the CAP

- **Effective 10/1/2024**
 - **R1** - ECWT and unit cold weather information
 - **R2** - Applicable to generating units with a commercial operation date **on or after October 1, 2027**
 - **R4** - Cold Weather Preparedness Plan (CWPP)
 - **R5** - Annual training on CWPP
 - **R6** - If a Generator Cold Weather Reliability Event (GCWRE) occurs, develop a CAP **w/ 150 days or July 1**, whichever is earlier
 - **R7** – Timelines for the completion of Corrective Action Plans
 - **R8** – Generator Cold Weather Constraint declarations
- **Effective 10/1/2025**
 - **R3** - Applicable to generating unit(s) in commercial operation **prior to October 1, 2027**

- EOP-012-2 Ballot Status
- Continued work on EOP-011 and TOP-002 revisions

A map of North America, including the United States, Canada, and Mexico. The map is stylized with different shades of blue and grey. A prominent horizontal band of medium blue color stretches across the middle of the map, passing through the United States. The text "Questions and Answers" is centered within this band.

Questions and Answers

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Facility Ratings Task Force

Update

Jeremy Harris, Evergy
MRO CMEP
July 26, 2023

RELIABILITY | RESILIENCE | SECURITY



- **Chair:** Tim Ponseti (SERC, VP of Operations)
- **Vice-Chair:** Jennifer Flandermeyer (Evergy, Director of Federal Regulatory Affairs)
- **NERC Liaison:** Al McMeekin
- **Sub-teams**
 - Implementation Guidance - Sustaining Accurate Facility Ratings
 - Support Project 2021-08 Modifications to FAC-008 Standard Drafting Team
 - Whitepaper on Sampling for Facility Ratings programs

- **Implementation Guidance for FAC-008-5**

- Provide examples and approaches on how entities can demonstrate compliance with the standard requirements
- Incorporate best practices used by entities to address factors such as:
 - Lack of Awareness
 - Inadequate Asset and Data Management
 - Inadequate Change Management
 - Inconsistent Development and Application of Facility Ratings Methodologies
- Build upon the 2017 MRO FAC-008-3 Standard Application Guide
 - Intend to coordinate to make sure that these documents don't contradict, but complement each other and provide consistent guidance to industry

- **Scheduled completion date: March 2024**

- Goal is to complete the document in November and present for consideration at December RSTC meeting
- Once Approved by the RSTC, the document would have to be considered for deference by ERO Enterprise CMEP staff

Co-leads: Robert Reinmueller (Hydro One) & Brian Evans-Mongeon (Utility Services)

Members:

- ❑ Curtis Crews (TexasRE)
- ❑ Curtiss Frazier (Ameren)
- ❑ Rajesh Geevarghese (Exelon Corp)
- ❑ Mike Guite (BC Hydro)
- ❑ David Jacobson (Hydro One)
- ❑ Jim Kubrak (Reliability First)
- ❑ Ryan Mauldin (NERC)
- ❑ Joseph Riebau (Constellation Power)
- ❑ Jim Uhrin (Reliability First)

- **Support Project 2021-08 Modifications to FAC-008 Standard Drafting Team**
 - Active participation in Project 2021-08 Modifications
 - Focusing FAC-008-6 on the most Limiting Element & next most Limiting Element
 - Clarifying the meaning of the term “jointly owned”
 - FAC-008 SDT has completed and submitted updates for posting and comments
 - Improving definitions, usage and capitalization of terms to provide clarity for other NERC Glossary of Terms used in the standard such as:
 - Facility vs facility
 - Element
 - Facility Rating, Equipment Rating, Rating
 - Develop diagrams to help provide guidance (similar to BES Reference document)
- **Scheduled completion date: March 2024**
 - Project 2021-08 – NERC RSTC August agenda for approval, and posting for comments in late August/Early September (45 day posting)
 - Working towards having proposed changes to Glossary of Terms and diagrams for submittal in comment period

Co-leads: Dre Pliodzinskas (Dominion Virginia) & Jeremy Harris (Evergy)

Members:

- ❑ Curtis Crews (TexasRE)
- ❑ Pamela Frazier (Southern Company)
- ❑ Rajesh Geevarghese (Exelon Corp)
- ❑ Ryan Mauldin (NERC)
- ❑ Joel Rogers (SERC)

- **Whitepaper on Sampling for Facility Rating programs**
 - Developing guide/best practices for stakeholders (not REs) for implementing sampling as a control
 - Sections
 - Introduction
 - Parameters which impact Facility Ratings
 - Assessing Risk
 - Methods for verifying Facility Ratings
 - Incorporating verification activities into a Facility Ratings program
 - ERO has a sampling handbook that looks at general sampling approaches for auditors to use when performing various compliance monitoring activities
- **Scheduled completion date: December 2023**
 - Targeting having a rough draft by end of August

Co-leads: Jennifer Flandermeyer (Evergy) & John Stephens (City Utilities of Springfield)

Members:

- ❑ Curtis Crews (TexasRE)
- ❑ Rajesh Geevarghese (Exelon Corp)
- ❑ Brad Harris (CenterPoint Energy – Reliability First)
- ❑ Kim Kubrak (Reliability First)
- ❑ Ryan Mauldin (NERC)
- ❑ Karen Onaran (Electricity Consumers Resource Council)
- ❑ Jon Radloff (American Transmission Company)
- ❑ Joseph Riebau (Constellation Power)
- ❑ Jim Uhrin (Reliability First)



Questions and Answers

Thank You!

Please Complete the 2023 Hybrid CMEP Conference Survey



<https://www.surveymonkey.com/r/JVM9VBQ>



CLARITY

ASSURANCE

RESULTS

CONFERENCE ORGANIZERS

MRO CMEP Advisory Council

Terri Pyle, Chair
Oklahoma Gas and Electric

Tiffany Lake, Vice Chair
Evergy, Inc.

Alison Archer
MISO

Ashley Stringer
Oklahoma Municipal Power Authority

Bryan Dixon
Xcel Energy

Carl Stelly
Southwest Power Pool

Eric Ruskamp
Lincoln Electric System

Kevin Lyons
Central Iowa Power Cooperative

Larry Heckert
Alliant Energy

Mark Buchholz
Western Area Power Administration

Matt Caves
Western Farmers Electric Cooperative

Nazra Gladu
Manitoba Hydro

Theresa Allard
Minnkota Power Cooperative

Troy Brumfield
American Transmission Company

MRO Staff

Richard Burt
Senior Vice President and Chief Operating Officer

William Steiner
Director of Compliance Monitoring

Michelle Olson
Compliance Monitoring Administrator

Jessie Mitchell
Director of Communications

Cris Zimmerman
Manager, Outreach and Stakeholder Engagement

Shawn Keller
Outreach Coordinator

Lauren McClary
Meeting Administrator



CONFERENCE CLOSING

Thank you all for attending this event!

Your feedback is very important to us. Please provide your feedback using the link or QR Code below or the link below:



<https://www.surveymonkey.com/r/JVM9VBQ>

Bill Steiner: william.steiner@mro.net – Compliance Monitoring

Michelle Olson: michelle.olson@mro.net – General Questions

