

JUNE 2021

**“If you want to build a ship, don’t drum up people together to collect wood and don’t assign them tasks and work. But rather, teach them to long for the endless immensity of the sea.”**

*- Antoine de Saint-Exupéry*

# MIDWEST RELIABILITY **MATTERS**

# Inside This Issue

- 3 CEO Message
- 5 Compliance Monitoring and Enforcement Program
- 11 External and Regulatory Affairs
- 12 Bulk Power System Reliability
- 17 Security Corner
- 20 Strategic and Financial Update
- 23 Diversity, Equity and Inclusion
- 26 Industry News and Events

## **DISCLAIMER**

MRO is committed to providing non-binding guidance to industry stakeholders on important industry topics. Subject matter experts from MRO's organizational groups have authored some of the articles in this publication, and the opinion and views expressed in these articles are those of the author(s) and do not necessarily represent the opinions and views of MRO.

## CEO MESSAGE



# The Power of Collaboration

## What we can accomplish when we work together

Two short months ago, the ERO Enterprise reached an important milestone with the Align and Secure Evidence Locker (SEL) projects when MRO, NERC, and Texas RE all went live with the new systems on March 31. WECC went live on May 10, and SERC, NPCC, and ReliabilityFirst followed shortly thereafter on May 24. This accomplishment is notable for a number of reasons. First, it demonstrates the commitment the ERO Enterprise made to address inconsistencies in Compliance Monitoring and Enforcement Program processes across the Regional Entities. The Align tool moves us all onto a common, standardized platform, providing for consistent application of CMEP activities and enhancing the effectiveness of how we execute statutory functions.

Second, in working with industry stakeholders to develop the Align Tool, the concept of Secure Evidence Lockers was introduced. The SEL provides a secure, isolated environment to collect and protect CMEP data - significantly reducing the risk of loss or exposure of evidence. The SEL was implemented to address stakeholder data security concerns, and while it did add to the cost and timeline of the project, the benefits to the entire ERO ecosystem are paramount. Needless to say, the final implementation of SEL could not be timelier, coming on the heels of a significant supply chain attack in December and an overall increase in cyber threats across the energy sector.

## CEO MESSAGE

Third, this project demonstrates the power of collaboration and what we can accomplish when we work together. The Align team is made up of individuals from across the ERO Enterprise who have dedicated a significant amount of time and effort to developing, testing, enhancing, and implementing these important tools. MRO staff worked diligently leading up to the go live date to prepare for and provide registered entities with the necessary information and training to ensure a successful launch. I want to take a moment to recognize their efforts, and to thank industry stakeholders for participating and providing input during the entire process. Your feedback was critical to a successful outcome—the end result would not have been the same without it.

This kind of collaboration isn't easy, and I continue to be impressed with how we have matured as organizations...as an enterprise...as an ecosystem. The time and effort we invested into transforming the way we work together and alongside each other, has laid the foundation for this accomplishment and will serve us well as we address the challenges of the future.

I also want to highlight another significant milestone for MRO. On May 10, we welcomed staff back to the office on a voluntary basis for the first time since the onset of the COVID-19 pandemic. When MRO's Emergency Response Team made the tough decision in March of 2020 to send staff home, we had no idea that it would be fourteen long months before we would have the opportunity to return. Throughout this time, many difficult decisions were made regarding how best to continue the important work we do while keeping the health and safety of our staff, our visitors, and our registered entities as the highest priority.

We took advantage of the office closure last year to remodel and expand our office space. The expansion allowed us to fully address pandemic restrictions and provide for a safe, healthy, and welcoming space for our staff and visitors. One of the most notable facility improvements is the installation of an HVAC bipolar ionization system, which is proven to help remove viruses like SARS-2-CoV from the air and provide a clean air environment.

With COVID-19 numbers decreasing and vaccination rates increasing, COVID-19 restrictions will hopefully soon be a thing of the past. I look forward to fully reopening the office in September, and to welcoming all of you to the new space as soon as it is safe to do so.

Until then, enjoy the longer days and the warm weather to come.

**Our future is bright!**

*-Sara Patrick, MRO President and CEO*

**“This kind of collaboration isn't easy, and I continue to be impressed with how we have matured as organizations...as an enterprise...as an ecosystem.”**

# COMPLIANCE MONITORING AND ENFORCEMENT PROGRAM



## ERO Enterprise Align and SEL Update

We are excited to announce that all Regional Entities are now live with Release 1 of the Align tool and the ERO Secure Evidence Locker (SEL). Align and the ERO SEL are designed to process and track all compliance monitoring and enforcement activities with the goal of improving security and standardizing processes on a common platform across the ERO Enterprise.

All registered entity staff seeking to access Align must register for an [ERO Portal](#) account. Each registered entity's Primary Compliance Contact (PCC) is responsible for approving access requests for their respective entity via the ERO Portal. All users who have been previously been granted access, as well as those granted access in the future, to the Align Submitter Role will have access to the ERO SEL. If you have questions or problems concerning your ERO Portal account, please submit a support ticket [here](#).

As we prepare for the upcoming Release 2 launch on July 19, 2021, the project team and regional subject matter experts (SMEs) are focusing on training materials that are currently in development, and Regional Entity and registered entity training sessions will be announced and held closer to the launch date.

### Release 2 Functionality Overview for Registered Entity Staff

- Technical Feasibility Exceptions (TFEs)
- Periodic Data Submittals (PDSs)
- Self-Certifications
- Attestations
- ERO SEL to include evidence submission for the above activities

Please visit the [NERC Training Site](#) for access to all Align and ERO SEL training materials, including training videos and user guides. Reach out to your MRO Regional Training Leads, Ryan McNamara and Michael Spangenberg at [align@mro.net](mailto:align@mro.net), with any Release 1 Align and ERO SEL-related access or training questions.

If you experience any technical issues, please submit a NERC help desk ticket [here](#).

- *Desirée Sawyer and Marissa Falco, MRO Align Change Agents*



## MRO HEROs and AskCMEPAC

### Our entity has a question...

One of the purposes of MRO and the MRO Compliance Monitoring and Enforcement Program Advisory Council (CMEPAC) is to conduct outreach and awareness to promote compliance.

In November 2016, the MRO Risk Assessment and Mitigation (RAM) Department began encouraging registered entities to submit questions relating to NERC compliance via email at [heros@mro.net](mailto:heros@mro.net). To date, RAM has received over 375 questions through the HEROs email. In August 2020, the CMEPAC established the [askcmepac@mro.net](mailto:askcmepac@mro.net) email address and monthly calls to assist registered entities in strengthening compliance programs, to discuss pending enforceable NERC Reliability Standards, and to field questions related to NERC compliance from a CMEPAC member perspective. Responses from the CMEPAC are not intended to determine if an entity is, or is not compliant, and may on occasion be forwarded to [heros@mro.net](mailto:heros@mro.net) with approval from the submitting entity.

One of the many items discussed within the CMEPAC and considered under the council's work plan is to coordinate with the RAM Department to periodically review and publish redacted questions posed to HEROs and askCMEPAC in the MRO Midwest Reliability Matters newsletter. Questions and responses from RAM staff through HEROs have been slightly altered to appeal to a wider range of entities. This month, we have three questions and responses to share.

#### **Question 1 (CIP-002-5.1a, CIP-005-6) to HEROs**

*A management system server may sit outside the ESP and initiate connections into the ESP through the firewall/EAP. While the firewall rules will allow user-interactive ports (SSH, RDP, etc.) through for the purpose of*

*scanning, the management system server will not possess credentials with the ability to change target system settings or affect target system operation. How should management systems such as this be classified? Exempt Cyber Asset, or Intermediate System/EACMS?*

**Response from RAM:** If the management system is not designed or configured to permit a user to interact with a BES Cyber System (BCS) and it can be demonstrated that a user is unable to interactively access the BCS remotely, then the vulnerability server/system can be determined to not have Interactive Remote Access (IRA). However, before determining that such a server/system is exempt from any CIP classification, ensure that all possible classifications are considered:

- Does the vulnerability server/system pose a 15-minute (misuse in particular) impact as a BCA?
- Does the vulnerability server/system perform electronic access control or electronic access monitoring of the Electronic Security Perimeter (ESP) or BCS (EACMS)?

As a best practice, MRO recommends that management systems such as vulnerability scanners, network management and monitoring systems, patch servers, backup systems, or any other type of computer management system that manages BCS directly from outside the ESP be protected as Intermediate Systems to mitigate security and compliance risks posed by inadvertent or malicious use of IRA. Web browsers, secure shell (SSH) utilities, Remote Desktop Protocol (RDP), and other interactive user utilities are commonly included as optional packages within operating systems and can be turned on inadvertently by users or maliciously by adversaries. The resulting security consequences can be serious or substantial when an actual risk scenario unfolds as a result, as has been demonstrated in recent supply chain compromises.

An alternate best practice (risk reducing approach) permitted by some management systems is to configure management systems to 'pull' (as with an agent) rather than 'push' changes. Management servers can be configured to respond to queries initiated from the inside of the ESP outbound, rather than driving change from outside the ESP inbound. Architecting the management implementation as a 'pull' can therefore limit risk by eliminating the potential for inadvertent or malicious use of IRA.

One approach to manage the risk of inadvertent or malicious IRA could be to add a detective control that alerts when IRA is initiated from a Cyber Asset that is designed for system to system process communication only. The inadvertent IRA may not be prevented (there is still potential for noncompliance), but the detective control would provide positive identification of the potential noncompliance, and mitigating activity could be pursued more immediately in response thereby limiting the duration.

## **Question 2 (PRC-027-1) to HEROs**

*If the baseline comparison identifies a deviation of 15% or greater, is it correct that we have until December 31, 2027 to complete the Protection System Coordination Study?*

**Response from RAM:** Looking at the three options stated under PRC-027-1 R2:

If an entity selects Option 2 for their initial performance of R2, then the establishment of the baseline must be prior to the effective date of 4/1/2021.

The Transmission Owner, Generator Owner or Distribution Provider must establish a fault current baseline. Fault current baseline values can be obtained from the short-circuit studies performed by the Transmission Planners, Planning Coordinators, or Transmission Owners as Generator Owners and Distribution Providers may not have or maintain short-circuit models. In a time interval not to exceed six-calendar years following the effective date of 4/1/2021, an entity must perform a fault current comparison (present fault current values to their established baseline). If the comparison identifies a deviation less than 15 percent, no further action is required for that six-

## COMPLIANCE MONITORING AND ENFORCEMENT PROGRAM

year interval; however, if the comparison identifies a 15 percent or greater deviation in fault current values (either three-phase or phase-to-ground) at each bus to which the BES Element is connected, the entity must also perform a Protection System Coordination Study during the same six-year interval (4/1/2021- 12/31/2027). The six-calendar-year time interval was selected as a balance between the manpower required to perform the studies and the potential reliability impacts created by incremental changes of Fault current over time.

If an entity selects Option 1 then performance of a Protection System Coordination Study must be completed in 2027 (a time interval not to exceed six-calendar years).

Option 3 is a combination of options 1 and 2.

### Question 3 (EOP-004-4) to AskCMEPAC

*This Reliability Standard has a Threshold for Reporting under Physical threats to its Facility, which in part states, "Physical threat to its Facility excluding weather or natural disaster related threats, which has the potential to degrade the normal operation of the Facility."*

*With the increasing amount of dispersed generation assets (wind and solar) Facilities that Entities are employing and Inclusion 14 of the BES definition, guidance is requested on the word "potential."*

*The simple definition (of this non-NERC defined) word is, "existing in possibility or capable of development into actuality."*

*Here are some examples. In both examples, the potential was present, if the bad actor continued with further acts. But entities don't know the intent of the bad actor.*

- 1. A solar Facility notes that a solar array was tampered with and disconnected but was not removed, does this require reporting? There was a potential to impact the Facility output (in this case the capacity was reduced by a small capacity output) but entities don't know what the intent of the bad actors were.*
- 2. A wind Facility notes that a turbine tower door was breached but there were no noted causes that would impact the Facility, does this require reporting.*

**Response from AskCMEPAC:** Deciding whether to report a potential physical threat to a facility can be a difficult decision. When deciding whether to report a potential physical threat to a facility one should always err on the side of reporting. In other words, when in doubt, submit the report. It may also be helpful to note that many companies have a defined process and a designated team that includes supervisor and management level personnel from System Operations and CIP who are responsible for deciding whether to report the potential threat in question.

1. For the first example, before making any decision one should verify that there were no recent maintenance activities that could explain why the solar array was disconnected. Assuming there was no justification found for the apparent tampering, it could be suspicious activity at the facility and an OE-417 would be submitted to the DOE, NERC, and MRO within 24 hours.
2. For the second example, based on the description provided, one could assume the "breach" was an intentional act of forced entry and one should proceed with submitting an OE-417 to the Department of Energy, NERC, and MRO within 24 hours.

*- Mark Buchholz, Compliance Manager with Western Area Power Administration and CMEPAC member, and Paul Melhaff, Manager of NERC Compliance with Sunflower Electric Corporation and CMEPAC member*

## About the Authors:



Mark Buchholz is a 1988 graduate of South Dakota State University. Following completion of a Bachelor of Science Degree in Electrical Engineering, he has been employed with the U.S. Department of Energy, Western Area Power Administration (WAPA) serving in various operations and maintenance positions at WAPA's Headquarters Office in Lakewood, CO: the WAPA-Upper Great Plains Region (WAPA-UGPR) South Dakota Maintenance Office; the WAPA-UGPR Maintenance Engineering Office; and the WAPA-UGPR Watertown Operations Office.

Since May 2010, Buchholz has served as a Compliance Manager for WAPA's Upper Great Plains Region and is a member of the NERC Compliance and Certification Committee; the Midwest Reliability Organization (MRO) CMEP Advisory Council; the Mid-Continent Compliance Forum (MCCF) Steering Committee; the MRO Performance Risk Oversight Subcommittee; and the Southwest Power Pool (SPP) Reliability Compliance Advisory Council.

Buchholz's duties as Compliance Manager include providing technical expertise to WAPA management and employees on NERC Reliability Standard compliance issues as they relate to power systems operation and maintenance, transmission planning, physical security, and cybersecurity. He serves as WAPA-UGPR's technical expert on the NERC Reliability Standards and provides internal guidance and outreach to WAPA employees on the interpretation of NERC Reliability Standards and their application to ensure WAPA-UGPR meets compliance with the requirements of the standards applicable to its registrations in the Eastern and Western Interconnections. Buchholz's duties also include oversight of the WAPA-UGPR System Operators Training Program and Facility Management of the Watertown Operations Office Complex.



Paul Mehlhaff has served as the Manager of NERC Compliance for Sunflower Electric Power Corporation since 2015. Prior to that he worked in the Transmission Engineering Department at as a Project Manager overseeing transmission-related design and construction activities. Before joining Sunflower in 2008, Mehlhaff spent nearly 20 years working for several manufacturing companies and holding numerous positions in engineering and operations.

Paul holds a bachelor's degree in Electrical Engineering from South Dakota State University, is a member of the MRO CMEP Advisory Council, and a member of the Midcontinent Compliance Forum Steering Committee.



# MRO TO HOST 2021 VIRTUAL CMEP CONFERENCE

July 27, 2021 | 9:00 a.m. to 4:00 p.m. Central | WebEx

## Conference Details

Midwest Reliability Organization's CMEP Advisory Council is pleased to announce it will host the Annual MRO Compliance Monitoring and Enforcement Program (CMEP) Conference, virtually, on July 27, 2021. The purpose of this conference is to provide registered entities valuable information on compliance monitoring and enforcement activities within MRO's footprint, as well as other important topics for the industry.

Compliance and enforcement professionals from registered entities within MRO's footprint are encouraged to participate - there is no fee for attendance.

## Planned Agenda Topics

- CIP Low Impact
- Compliance Risk
- Distributed Energy Resources
- Facility Ratings
- Internal Controls
- NERC CIP Open Projects
- Risk-Based Oversight and Monitoring and Compliance Oversight Plans
- Reliability and Security Risks
- Supply Chain

## Registration

To register to attend this event click [here](#). Registration closes on **July 25, 2021**.

## EXTERNAL AND REGULATORY AFFAIRS

# State Regulatory Outreach Initiative

How is it summer already? Unlike the slow pace of last year, this year seems to be moving at an unusual speed. As mentioned in the April issue of the newsletter, the ERO Enterprise began an initiative to increase awareness and share information with state regulators to inform these individuals of standards and publicly available reliability and security information and enhance visibility within the states about ERO Enterprise work. Developing relationships and sharing information on risks to reliability and security of the North American bulk power system across these regulatory agencies is critical to our success.

The latest communication sent to state regulatory agencies informed them of NERC's recently released [NERC Summer Reliability Assessment](#) (SRA), including this one page [SRA infographic](#). Additionally, I introduced the state commissions to the MRO Security department and invited Commissioners and staff to attend both the Reliability Conference and the Security Conference, to be held later this year. This state outreach initiative will continue to have touch points with the state regulatory offices and provide publicly available information and answer questions as received.

### Regulatory Update

At the May 20, 2021, Federal Energy Regulatory Commission (FERC) virtual open Sunshine meeting, FERC staff presented the [2021 Summer Energy Market and Reliability Assessment](#). Key findings that FERC staff presented at the meeting include, "all NERC planning regions should have enough generation available to exceed their reserve margins, but many regions would face challenges in extreme conditions." The report stated that temperatures are forecasted to be higher than average this summer and that the continued economic effects of the COVID-19 pandemic add to demand uncertainty. Additionally, the risks of drought conditions and wildfires lead to the uncertainty of summer resource demand. FERC staff expanded the report to include September, as high heat events have occurred in September in previous years. For more information, you can find the report [here](#).

Also, at the May 20, 2021, FERC virtual open Sunshine meeting, the Commissioners commented on the Colonial Pipeline System Cyber Attack, expressing the need for mandatory standards in the pipeline industry and, after extended discussion surrounding proposed amendments, approved two natural gas projects. The next FERC virtual open Sunshine meeting will be held June 17, 2021, at 9:00 AM (CDT) and information about that meeting can be found [here](#). Upcoming FERC Technical Conferences, including the June 23-24, 2021, [Technical Conference to Discuss the Resource Adequacy Developments in the Western Interconnection](#) can be found [here](#).

If you have any questions, do not hesitate to reach out to me at [tasha.ward@mro.net](mailto:tasha.ward@mro.net).

- Tasha Ward, Director of Enforcement and External Affairs

# BULK POWER SYSTEM RELIABILITY



## Assessing the Aggregated Impacts of Distributed Energy Resources

The location of electric generation resources across North America is under significant change due to decarbonization policies, modernization, and cost-effective emerging technology solutions being more readily available to end customers. Additionally, placement of generation geographically closer to end users is an attractive concept for significantly lowering “line loss” potential. Distributed Energy Resources (DERs) range from renewables like wind turbines and solar photovoltaic panels, to conventional generators like diesel or natural gas electric power generating resources. Distribution-connected generating resources are subject to different policies or regulations at the local, state and federal levels than traditional centrally located ones.

The North American Electric Reliability Corporation (NERC), under its efforts in the NERC Distributed Energy Resource Task Force (DERTF) and NERC Essential Reliability Services Task Force/Working Group (ERSTF/ERSWG), addressed critical goals, including some associated with the Electric Reliability Organization (ERO) Enterprise Operating Plan. Based on several technical discussions, DERTF, ERSTF and ERSWG guided initial DER

data collection and impact evaluations. The impact identified under DERTF, ERSTF, and ERSWG paved the way for the industry to continue work under the NERC assembled “System Planning Impacts from Distributed Energy Resources Working Group” (SPIDERWG) in December 2018.

The NERC SPIDERWG’s task is to evaluate and address the impacts of distributed resources on bulk power system planning, modeling and reliability. The SPIDERWG consists of subject matter experts from various industries with diverse DER, system planning and reliability assessment expertise. SPIDERWG deliverables include creating reliability guidelines on system planning, reliability impacts, data collection and information sharing.

Additionally, SPIDERWG will recommend DER modeling improvements, MOD-032 DER inclusion, IEEE Standard 1547-2018 adoption, and additional educational materials. Due to the broad range of deliverables from DERs, SPIDERWG created four subgroups — modeling, verification, coordination, and studies — to lead the charge for developing the deliverables. For additional information, review the SPIDERWG scope, activities and meeting materials posted on [NERC’s website](#).

In 2020, the SPIDERWG determined it would be beneficial to perform a comprehensive review of all NERC Reliability Standards to identify potential gaps or improvements for DER impacts. To accomplish this, the SPIDERWG Coordination subgroup volunteers reviewed the majority of currently enforced reliability standards, identified potential gaps or improvements, and presented the essential findings and recommendations from that review in a white paper. The paper organizes the potential gaps and improvements based on high, medium and low levels. Gaps or improvements identified as high are likely to lead to a potential reliability gap that should be addressed promptly. As a medium, increasing DERs may show entities have potential reliability issues if the standards are not updated to address the problems identified. As a low, gaps and areas for improvement relate to clarity and consistency regarding how DERs would impact the bulk power system. The white paper provides the review approach and additional details in Appendix A. Currently, the SPIDERWG is performing final reviews for the whitepaper and anticipates seeking NERC Reliability and Security Technical Committee (RSTC) approval in 2021.

- Sunny Raheem, Supervisor of System Planning Modeling, SPP

## About the Author:



Sunny Raheem is a supervisor of system planning modeling at South-west Power Pool (SPP) in Little Rock, Arkansas. He has more than ten years of transmission modeling and generator interconnection experience and is a registered professional engineer (P.E.) in Arkansas. Sunny has both master’s and bachelor’s degrees in systems engineering from the University of Arkansas at Little Rock. He has experience in power system modeling and analysis, including steady-state and dynamic model development and simulations. In his current role, Sunny is involved in managing and coordinating NERC compliance modeling requirements for the reliability standards applicable to Planning Coordinator (PC) functions for SPP. Sunny also participates and represents the MRO region on the NERC SPIDERWG.

# MRO to Publish Regional Summer Assessment

MRO annually reviews, evaluates, and assesses the bulk power system in the Planning Coordinator (PC) and Reliability Coordinator (RC) areas within the MRO region for reliability purposes. MRO's Reliability Analysis team is planning to publish a 2021 Regional Summer Assessment (2021 RSA) in June that reviews the generation resource performance from the 2020 summer season to identify trends and evaluate resources and transmission system adequacy needed to meet projected demand for the upcoming summer season. The 2021 RSA also evaluates operational readiness in the MRO region to report potential resource and transmission system adequacy concerns that have the most impact on system reliability. The assessment reflects MRO's independent evaluation and is intended to inform industry leaders, planners, operators, and regulatory agencies, to better prepare them to take necessary actions to ensure bulk power system reliability.

Generation resource performance and availability is key to meeting the projected upcoming summer demand in the MRO region. Rapidly changing resource mix and increased levels of renewable energy resources could create significant challenges for operators and planners, particularly with inaccurate real-time wind forecasting. The assessment utilizes the generating equipment information collected in the Generating Availability Data System (GADS) to analyze generation performance and causes of system outages. It identifies the failure risks on each type of generation, as well as system improvements that can be implemented by owners and manufacturers to reduce the forced outage rates. The generating unit monthly performance data collected in GADS is also used to analyze trends in the changing resource mix to provide meaningful information for resource adequacy analysis and planning.

The 2021 RSA also compares the previous 3-year summer, normal and extreme projected load, the actual load, and the all-time summer peak load for each PC in the MRO region, and provides an outlook on the upcoming summer season. The accuracy of the outlook is related to many factors that could impact the summer resource availability. The 2021 RSA provides seasonal forecast based on the anticipated summer resources and assumed peak demand, the extreme low generation and extreme peak demand scenarios. Under the extreme peak demand and extreme low generation scenario, some areas may have to issue Energy Emergency Alerts (EEAs) and take mitigating actions to ensure the system maintains reliability.

The Transmission Availability Data System (TADS) collects transmission equipment (100kV and above) availability data and the Misoperation Information Data Analysis System (MIDAS) collects transmission equipment Misoperation data. The summer assessment analyzes the transmission outages and protection system misoperations experienced during the summer of 2020 in order to predict future transmission system availability.

Event Analysis (EA) is a critical process for analyzing bulk power system disturbances, which include severe system faults, equipment failures, and human performance errors. The purpose of the EA program is to determine the causes of those disturbances, and evaluate any potential lessons learned to share with industry. The 2021 RSA reviews Bulk Electric System events and EA data from the previous year, and identifies meaningful trends that need to be corrected or mitigated. This assessment also provides a special evaluation of the potential impacts of the COVID-19 pandemic based on the previous summer peak demand and the 2021 seasonal forecast.

The 2021 RSA is an independent assessment that focuses on finding potential operational concerns in the MRO region that may need to be addressed for summer 2021. The assessment supports MRO's strategic goal of Identification and Assessment of Emerging Reliability Risks, and compliments [NERC's 2021 Summer Reliability Assessment](#).

- Dianlong Wang, MRO Senior Power Systems Engineer

# Increasing Awareness of Reliability Risk

## The important work of MRO's Reliability Advisory Council

MRO's Reliability Advisory Council (RAC) hit the ground running this year with the approval of its 2021 work plan by the board's Organizational Group Oversight Committee (OGOC). The work plan consists of seven items primarily focused on conducting outreach, supporting the development of the MRO Regional Risk Assessment (RRA), and the implementation of a matrix tool for prioritizing risks to the regional bulk power system. The work plan is built around the MRO Strategic Plan and Metrics, emerging regional risks, and outreach to raise awareness and increase reliability. Below is more detail on a few of the items mentioned above.

### Conduct Outreach and Awareness

In 2020, the RAC was responsible for hosting one major conference, two webinars (one was hosted by the Protective Relay Subgroup), and authoring multiple newsletter articles. In 2021, the RAC is planning its annual Reliability Conference scheduled for August 24, with potential topics on Electric Gas Coordination, Facility Ratings Best Practices and Seasonal Coal Plant Operations. There is also a Regional Winter Preparedness Workshop being developed for late Q3 or early Q4. The council has already contributed four articles for the MRO "Midwest Reliability Matters" newsletter in 2021.

### Support the Development of the 2022 MRO Regional Risk Assessment (RRA)

While the RAC has always provided input in the identification of reliability risks in the region, this year two RAC members will support MRO staff in ranking risks for the 2022 RRA utilizing the new Reliability Risk Matrix – a tool created by the RAC to help prioritize risk. Having council members help staff rank risks using the risk matrix is a new process that will be implemented in 2021.

### Implement a Matrix Tool for Prioritizing Risks

In 2019, the RAC developed the Reliability Risk Matrix and shared this with the OGOC and the other two MRO advisory councils in 2020. The matrix tool was later used to rank both security risks and operations and planning risks in the [2021 MRO Regional Risk Assessment](#). The matrix ranks the risk by looking at the consequence/impact, which can range from negligible to severe, then the likelihood, which ranges from very likely to almost certain. These two categories result in a risk ranking of Low, Medium, High or Very High.

The RAC is committed to informing MRO registered entities on important industry planning and operational developments and concerns. Please consider registering for the upcoming August 24, 2021 Reliability Conference.

If you have any questions regarding the conference, please contact [Dana Klem](#). The complete 2021 work plan can be found [here](#). If you have any questions, please contact [Bryan Clark](#), MRO Director of Reliability Analysis and RAC liaison.

- Dick Pursley, Director of Operations, Great River Energy and Reliability Advisory Council Chair, and Bryan Clark, MRO Director of Reliability Analysis, RAC Liaison

		Reliability Risk Matrix				
		Likelihood (L)				
		L1	L2	L3	L4	L5
Consequence/Impact (C)		Very Unlikely	Unlikely	Possible	Likely	Almost Certain
C5	Severe	Medium	High	High	Very High	Very High
C4	Major	Medium	Medium	High	High	Very High
C3	Moderate	Low	Medium	High	High	High
C2	Minor	Low	Low	Medium	Medium	High
C1	Negligible	Low	Low	Low	Medium	Medium

# MRO TO HOST 2021 VIRTUAL RELIABILITY CONFERENCE

August 24, 2021 | 9:00 a.m. to 3:30 p.m. Central | WebEx

## Conference Details

Midwest Reliability Organization's Reliability Advisory Council is pleased to announce it will host the 2021 Reliability Conference via WebEx. This one-day conference will focus on Bulk Electric System (BES) reliability topics across the industry and specific to the MRO region.

Technical staff, subject matter experts, and power system engineers from registered entities are encouraged to attend this free conference.

## Planned Agenda Topics

- Electric Gas Coordination
- Facility Ratings Best Practices
- 2021 Cold Weather Events
- Canadian Provincial Grid Code Review

## Registration

To register to attend this event click [here](#). Registration closes on **August 23, 2021**. WebEx information will be provided once you have completed registration.

## SECURITY CORNER



# Securing Substations

## Cyber and physical security best practices

### Cyber Security at Substations

When it comes to cyber security for electric substations, we can learn from what is occurring in other industries. Over the last few months we've seen attacks on water treatment plants, and more recently the Colonial Pipeline – the largest pipeline system for refined oil in the U.S. We've all been inundated by vendors claiming that if company X had been using their solution then they wouldn't have been affected. Don't get caught up in the fear, uncertainty and doubt (FUD) being touted by these salespeople. The best approach to dealing with these kinds of scenarios is to establish a plan based on your known risk. Here are a few steps you could add to your plan:

1. Know your environment - Understand what “normal” and “abnormal” look like and ensure that your organization is able to respond.
2. Limit remote access - Remote access is a double edged sword. It can be really valuable and enable additional productivity, but it can also increase risk. If you have remote access, ensure that you're using a modern, supported, enterprise-class tool. Ensure you have role-based access and monitoring.
3. Use Multi Factor Authentication (MFA) - If you must have remote access, make sure that you enable MFA. We've seen credential stuffing and phishing play a central role in multiple breaches. MFA greatly lowers your risk.
4. Ensure that you have recoverable (and CLEAN) backups - Keeping track of your current device configurations and maintaining solid backups can be a major benefit in the event of a breach or ransomware attack. As part

## SECURITY CORNER

of this process, make sure that you've tested your ability to restore from backup. It does no good for anybody to perform backups if those backups cannot be used to recover information.

5. Test your incident response plan - It's imperative that everyone with a role in your incident response process has clarity on their role, knows what steps need to be taken, and that your entire organization tests that process regularly.

## Physical Security at Substations

When it comes to physical security of substations, the increase of copper prices, turbulent times and just good business practices...it is good to know that basic physical security practices still apply and are a good mitigation strategy for preventing unauthorized entry.

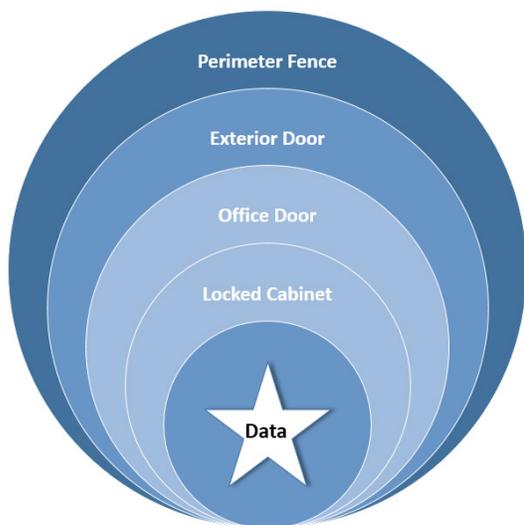
### Crime Prevention Through Environmental Design (CPTED):

- Natural Surveillance - Lighting, landscape, architecture. The objective is to "see and be seen".
- Natural Access Control - Walkways, fences, signage, lighting and landscape to clearly guide people and vehicles to and from the proper locations.
- Territorial Reinforcement - Public areas clearly distinguished from private areas. Owners are more likely to challenge intruders because they have a vested interest in the property.
- Maintenance - Neglected and poorly maintained areas are often grounds for criminal activity.

### 4 "D's" and a couple of "R's":

- Deter – Visual deterrents such as lighting, signage, visible security systems, vegetation control, security officer presence.
- Deny/Delay – Fences, lockable gates & windows, natural features, CPTED protection, security screens and quality locks.
- Detect – Alarm systems, cameras, personnel.
- Respond – Alarms, lights, voice, security staff, law enforcement and security escalation plans.
- Recover – Emergency response, disaster recovery, business continuity, crisis management.

## Defense in Depth:



## Zones/Layers of Protection:



Ultimately, all concepts/strategies implemented before design, with hardened and redundant systems!

- Jason Nations, Director of Enterprise Security, Oklahoma Gas and Electric and MRO SAC Chair, and John Breckenridge, Crisis Management Program Manager, Evergy, and MRO SAC Vice Chair

## About the Authors:



Jason Nations is Director of Enterprise Security at Oklahoma Gas and Electric Energy Corp., the parent company of OG&E, an investor owned utility headquartered in Oklahoma City, Oklahoma. He has extensive experience across multiple industries including energy, government and healthcare. In his current role, he oversees all cybersecurity efforts including both OT and IT. Jason started his utility career as part of OG&E's award-winning Smart Grid deployment. He has a BA and MS from Baylor University as well as several industry certifications.

Nations serves as chair of MRO's Security Advisory Council.



John Breckenridge is the Crisis Management Program Manager for Evergy based in Kansas City, MO. In his current capacity, he is responsible for the enterprise-wide crisis management program, business continuity planning, travel security, insider threat program, intelligence/counterintelligence and government/industry liaison. Additional responsibilities include strategic physical security support and security compliance. To be effective, Mr. Breckenridge uses his 30 plus years of military, criminal justice and industrial security experience to work with each functional department and business unit. Breckenridge began his career while in the US Army, where he was instrumental in supporting many special security operations throughout the US and in many countries, especially during his assignment in Europe.

In addition to his eight-year career in the military, Breckenridge worked for six years in the Jackson County, MO. criminal justice system. During this time, he specialized in security systems, close protection operations and special event security functions first with the Department of Corrections and then in conjunction with the Jackson County Courts. From 1993 until 2008, he was the Director of Security and Chief Security Officer for Aquila Energy until Aquila was purchased by Kansas City Power & Light (KCPL). Since this time Breckenridge has served in many security management capacities within KCPL and continuing with the merger creating Evergy in 2018.

Breckenridge is Board Certified in Security Management as a Certified Protection Professional, holds a BLA degree and a degree with an emphasis in Criminal Justice, is a Licensed Private Investigator.

He is also the past co-chairman and founding member of the NERC EISAC Physical Security Advisory Group, was a member of the NERC CIP014 Standards Drafting Team, served as a co-chairman for the NERC GridEx exercise design team, has served on the NERC Critical Infrastructure Protection Committee for 15+ years, and serves on multiple boards including; the Coast Guard's Area Maritime Security Council, the FBI's Domestic Security Advisory Council and the Kansas City Crime Stoppers TIPS Hotline and the vice chair of MRO's Security Advisory Council.



## Confronting the Energy Assurance Challenge

Six months ago, I found myself looking forward to 2021; anticipating a return to pseudo-normalcy as glimpses of a post-COVID world were becoming apparent, moving past the August 2020 Derecho storms that heavily impacted our region, and appreciating the completion of restoration efforts related to Hurricane Laura. However, as I write this from my home office not long after experiencing a supply chain compromise in December and Winter Storm Uri in February, I'm acutely aware that 2021 is also going to present us with new and challenging opportunities. These most recent events are likely some of the most impactful in the grid's evolutionary history and have reminded me again of how dynamic our industry has become (a far cry from how it was described when I joined it in the 1990s). It also emphasizes the need for us to focus directly on activities that can positively impact reliability and minimize future impacts of similar events.

Early observations of the February 2021 cold weather event, lessons learned from previous extreme weather events (both hot and cold), as well as forward-looking assessments of the grid, all point to energy assurance being the top reliability challenge requiring our attention. There are many facets of energy assurance that

have become common phrases in our industry – the changing resource mix, intermittent resources, behind-the-meter generation, transmission deliverability, shrinking reserve margins, and many others. I believe a large percentage of these are more easily addressed if we begin by focusing our efforts on energy assurance.

Simply put, how sure are we that energy will be available to serve load at any given time? One thing is for certain - we are a lot less sure than we once were, regardless of the timeframe being seasonal, long-term, or operational.

This is a complex problem due to the many variables involved in the equation. I'll posit that the most challenging aspect is that it requires us to revisit some of the common assumptions fundamental to how we plan and operate the system (things many of us learned in Power Systems 101):

- Is “capacity” a relevant concept anymore?
- What is the value of utilizing “reserve margins” for planning and operations, as currently calculated?
- What assumptions are we using in 50/50 and 90/10 scenarios and are they really 50/50 and 90/10?
- What does a transmission system even look like when it's no longer an electron interstate between large baseload generators and load centers?
- Is it possible that the most common “n-1” contingency for many portions of the Bulk Electric System is actually loss of a natural gas pipeline and not a generation or transmission element?

The ERO Enterprise and industry are looking hard at these complex questions and how to effectively provide energy assurance in the highly reliable bulk power system of the future. Most notably, NERC recently established the [Energy Reliability Assessment Task Force](#) (ERATF) to assess risks associated with unassured energy supplies, including the timing and variable output from renewable energy resources, fuel location, and volatility in forecasted load, which can result in insufficient amounts of energy on the system to serve electrical demand. ERATF meetings are open to industry participation.

MRO strongly supports the mission of the ERATF and will follow its work closely. In the [2021 MRO Regional Risk Assessment](#), “Uncertainty of Planning Reserve Margins” was identified as the highest risk to reliability within our region. We are in the process of identifying further actions to mitigate this risk, which aligns well with the work of ERATF. MRO's Reliability Advisory Council (RAC) is focused on risks to reliability, including energy assurance. All MRO RAC meetings are also open to public participation and the RAC will sponsor the [2021 MRO Reliability Conference](#) on August 24, which will include speakers and information relevant to industry in addressing this risk.

Additionally, the load shedding that took place during February of 2021 as a result of Winter Storm Uri led to a FERC-led inquiry, which MRO is a part of with NERC and other Regional Entities. That team seeks to understand not just the causes of generation outages, but also the more holistic energy assurance problems that led to large amounts of load shed for long durations of time in some areas. Lessons learned from this inquiry will be another source of context for the ERO Enterprise and industry as we all work together to ensure that reliability is not degraded as the bulk power system continues its transformation.

Thus far, 2021 has proven that although the problems we face may change, there will be ever present challenges in the pursuit of our shared vision of a reliable and secure North American bulk power system. The ERO Enterprise model provides a highly collaborative structure that allows us to combine our efforts to

address complex risk. Energy assurance is one of the most difficult challenges we will address, but working through this process together will undoubtedly be exciting and transformative.

Please consider participating in these efforts by getting involved with the NERC ERATF or [MRO RAC](#).

- Richard Burt, Senior Vice President and Chief Operating Officer

## Draft 2022 Business Plan and Budget Update

The [Draft 2022 MRO Business Plan and Budget](#), initially reviewed with board members in April, was posted for stakeholder comment on May 12, following endorsement by the Finance and Audit Committee during its second quarter committee meeting. The MRO Board of Directors is scheduled to vote on the proposed budget at its open meeting on June 24, 2021. MRO, along with NERC and the other Regional Entities, also presented highlights of their respective budgets to the Federal Energy Regulatory Commission (FERC) and NERC's Finance and Audit Committee. The budgeted costs reflect MRO's investment in its strategic objectives, which are aligned with the ERO Enterprise long-term strategy and will allow MRO to meet its delegated responsibilities.

The final version of the business plan and budget will be submitted for approval to the NERC Board of Trustees at its August meeting. Subsequently, NERC will file the business plans and budgets for NERC and the six Regional Entities with FERC in the fall.

- Regina March, Senior Accountant

## Employee Spotlight:

Congratulations to [Dr. Mike Bocovich](#), Principal Systems Protection Engineer at MRO, who will retire on July 7, 2021. Dr. Bocovich has been a dedicated member of MRO's Reliability Analysis team for the past four years, and his extensive industry experience and knowledge will be hard to replace. "Mike's positive attitude, willingness to help others, and depth of expertise will definitely be missed," said Director of Reliability Analysis Bryan Clark. "We wish him well in his future endeavors."

**MRO is hiring!** To apply, visit the [Careers Page](#) on our website or visit us on [LinkedIn](#).

## DIVERSITY, EQUITY AND INCLUSION AT MRO



### Celebrating the Month of June

*The month of June is a reminder to all of us that awareness and education are the keys to understanding and overcoming differences.*

The LGBTQ (Lesbian, Gay, Bisexual, Transgender, and Queer) community, sometimes expanded to LGBTQIA+ to include intersex and asexual, celebrates Pride Month during the month of June each year to commemorate the tipping point in queer history. The Stonewall Uprising lasted six days in Manhattan, New York. Members of the LGTBQ community held demonstrations in response to a police raid at the Stonewall Inn. This event has long since been a pivotal moment in the LGBTQ movement and the fight for civil rights. Although it did not start the gay rights movement, it was a driving force for activism. During the 1960's it was illegal to engage in LGBTQ behavior leading to constant harassment. After the Stonewall Uprising organizations such as the Human Rights Campaign (HRC), GLAAD, and PFLAG formed to help lead the LGBTQ political activism movement.

On the one-year anniversary of the Stonewall Uprising, June 28, 1970, an assembly took place on Christopher Street, now known as Christopher Street Liberation Day. Every year during the month of June, LGBTQ Pride takes place in many cities across the global to celebrate the birth of the liberation movement and the change that the Stonewall riots has brought to our culture. One of the most prominent symbols in the LGBTQ community is the rainbow pride flag created by Gilbert Baker (American Artist, gay rights activist, and United States Army Veteran) which includes 6 colors: red for life, orange for healing, yellow for sunlight, green for nature, blue for harmony and violet for spirit. This month take a moment to do some research and reflect on President Obama's words from his second inaugural address, "We, the people, declare today that the most evident of truths – that all of us are

created equal – is the star that guides us still; just as it guided our forebears through Seneca Falls and Selma and Stonewall.... Our journey is not complete until our gay brothers and sisters are treated like anyone else under the law – for if we are truly created equal, then surely the love we commit to one another must be equal as well.”

Juneteenth is another nationally celebrated diversity and equality commemoration. Specifically celebrating the end of slavery in the United States. Major General Gordon Granger issued General Order No. 3 on June 18, 1865, by the Union Army with a proclamation that would end slavery and free tens of thousands of African-Americans in Texas, closing the door on one of the last chapters of slavery in the United States. The General Order stated, “The people of Texas are informed that, in accordance with a proclamation from the Executive of the United States, all slaves are free. This involves an absolute equality of personal rights and rights of property between former masters and slaves, and the connection heretofore existing between them becomes that between employer and hired labor. The freedmen are advised to remain quietly at their present homes and work for wages. They are informed that they will not be allowed to collect at military posts and that they will not be supported in idleness either there or elsewhere.”

Juneteenth traces its origins back to Galveston, Texas, where Union soldiers, led by Major General Granger landed in the city with news that the Civil War had ended and slaves were now free. His announcement of the General Order followed Abraham Lincoln’s Emancipation Proclamation on January 1, 1863, outlawing slavery in Texas and other southern states who were rebelling against the Union for roughly two and a half years after President Lincoln’s Emancipation Proclamation that freed slaves in Confederate states. However, since the proclamation was made during the Civil War, it was ignored by Confederate states and it was not until the end of the war that the Executive Order was enforced in the South.

Today, Juneteenth symbolizes freedom and achievement. In fact, Texas was the first state to recognize Juneteenth



*Photo by Heather Mount on [Unsplash](#).*

as an official state holiday with roughly 47 other states recognizing Juneteenth. Let this day and every other day be a reminder that self-awareness and education about diversity and inclusion is not only important for the future of the ERO enterprise, but our country as well.

Another significant event that happened in June is the 1921 attack on Greenwood, which is one of the most significant events in Tulsa, Oklahoma history. Following World War I, Tulsa was recognized nationally for its affluent African American community known as the Greenwood District. This thriving business district and surrounding residential area was referred to as “Black Wall Street.” During the Tulsa Race Massacre, which occurred over 18 hours from May 31 to June 1, 1921, a white mob attacked residents, homes and businesses in the predominantly Black neighborhood. The event remains one of the worst incidents of racial violence in U.S. history. Sadly, the event is unknown to many of us as news reports were largely squelched, despite the fact that hundreds of people were killed and thousands left homeless.

There is much for us to learn from and embrace in the month of June. MRO acknowledges how important diversity, equality, and inclusion is, which is why we live by the vision and mission of our D&I committee: Celebrate the community within MRO by promoting awareness related to diversity and inclusion, and enhancing respect for others by acknowledging the importance of equity.

***Our future is bright!***

*- Holly Haynes, Sr. CIP Compliance Auditor, and Sara Patrick, President and CEO, on behalf of MRO's Diversity and Inclusion Committee*

## Industry Tips and Lessons Learned

NERC publishes [lessons learned](#) on its website designed to convey information gleaned from various NERC and Regional Entity activities. The lessons learned are not intended to establish new requirements under NERC Reliability Standards or to modify the requirements in any existing Reliability Standards. Compliance will continue to be determined based on language in the NERC Reliability Standards as they may be amended from time to time. Implementation of these lessons learned is not a substitute for compliance with requirements in NERC's Reliability Standards.

One new lesson learned has been published since the last MRO newsletter:

- [Interconnection Oscillation Disturbances](#)

In addition to lessons learned, NERC publishes Compliance Guidance to help industry and ERO Enterprise CMEP staff develop a common understanding for how compliance can be achieved and demonstrated. More information on how Compliance Guidance is developed, along with ERO Enterprise endorsed guidance documents can be found on the [Compliance Guidance](#) page of NERC's website.

# INDUSTRY NEWS AND EVENTS

## LATEST NEWS:

### FERC Submits FY 2022 Congressional Budget Justification

The Federal Energy Regulatory Commission (FERC) submitted its FY 2022 budget request to Congress, which includes FY 2021 Annual Performance Plan and FY 2020 Annual Performance Report. See the [full announcement](#).

### FERC Order 871 Clarity & Pipeline Cybersecurity Standards

Read the full FERC Issight, Volume 5 [here](#).

### FERC Publishes Hybrid Resources White Paper

The information in this white paper was developed through the Commission's July 2020 Hybrid Resources technical conference in Docket No. AD20-9-0001 and the post-conference comments. The technical conference focused on the growth of co-located hybrid and integrated hybrid resources and the current approaches to interconnecting such resources and allowing for their participation in the Regional Transmission Organization (RTO) and Independent System Operator (ISO) markets, as well as outside of RTO/ISO markets. Read the White Paper on [FERC's website](#).

### FERC 2021 Summer Energy Market and Reliability Assessment

The FERC Summer Assessment is divided into two main sections—the first on notable market conditions and the second on market fundamentals. The first section highlights three major areas of consideration ahead of summer 2021: summer readiness efforts, expected North American Electric Reliability Corporation (NERC) regional reserve margins, and western energy markets topics. Read the assessment on [FERC's website](#).

### NERC Summer Assessment Warns of Potential Energy Shortfalls

NERC's 2021 Summer Reliability Assessment

warns that parts of North America are at elevated or high risk of energy shortfalls this summer during above-normal peak temperatures. Read the [full announcement](#).

### NERC Releases Second Episode of Quarterly Compliance Podcast

NERC announced the release of the second installment of its quarterly compliance podcast, "Currently Compliant." Hosted by ERO Enterprise subject matter experts (SMEs), "Currently Compliant" is intended to be a quick way to bring attention to frequently asked questions on which the SMEs have some clear insights to share. Read the [full announcement](#).

## INDUSTRY EVENTS:

### NERC Industry Webinar: BPS-Connected Battery Energy Storage Systems and Hybrid Power Plants

July 15, 2021 | 1:00 to 3:30 p.m. Eastern

The NERC Inverter-Based Resource Performance Working Group (IRPWG) recently published Reliability Guideline: Performance, Modeling, and Simulations of BPS-Connected Battery Energy Storage Systems and Hybrid Power Plants. The guideline provides recommended performance characteristic for BPS-connected BESSs and hybrid plants that Generator Owners and project developers should consider. Register [here](#).

### NERC Board of Trustees and Member Representatives Committee Meetings

August 11-12, 2021 | WebEx

The third quarter NERC Board of Trustees and Member Representatives Committee meetings will be held virtually by WebEx. Registration will be available [here](#).

### Save the Dates for NERC's GridSecCon

October 19-20, 2021 | Virtual

NERC and Texas RE are co-hosting the 10th grid security conference, GridSecCon, on October 19–20, with training opportunities available on October

18. GridSecCon brings together cyber and physical security leaders from industry and government to deliver expert training sessions, share best practices, present lessons learned, and share effective threat mitigation programs. The event will be held virtually due to the ongoing pandemic. More details will be made available on the [E-ISAC website](#), [NERC website](#), and [Texas RE website](#).

We look forward to seeing you there virtually. For more information or assistance, please contact [events@eisac.com](mailto:events@eisac.com).

## REGIONAL AND MRO EVENTS:

### MRO CMEP Advisory Council Monthly Call

June 8, 2021 | 3:00 p.m. Central

The purpose of this call is to provide advice and counsel on topics such as the development, retirement, and application of NERC Reliability Standards, risk assessment, compliance monitoring, and the enforcement of applicable standards. Register [here](#).

### MRO RAC Q2 Meeting

June 9, 2021 | 8:00 a.m. to 4:00 p.m. Central

The Reliability Advisory Council will meet by WebEx on June 9 at 8:00 a.m. Central. Register [here](#).

### Industry Webinar: The SCOOP on Insider Threats

June 15, 2021 | 9:00 a.m. to 12:00 p.m. Eastern

SERC is hosting a webinar on insider threats for individuals responsible for cyber and physical security within their organizations. Read more and register [here](#).

### Industry Webinar: Maintaining Cyber Resiliency Through Simulation-Based Scenarios and Exercises Specific to the Energy Sector

June 17, 2021 | 11:00 a.m. Central

MRO and SERC are pleased to announce a joint webinar on maintaining cyber resiliency through simulation-based scenarios and exercises specific to the energy sector. Read more and register [here](#).

### MRO Q2 OGOC Meeting

June 23, 2021 | 8:30 a.m. Central

This is an open meeting of the board's Organizational Group Oversight Committee. Agenda materials and registration information is [here](#).

### MRO Q2 SAC Meeting

June 23, 2021 | 9:45 a.m. Central

This is an open meeting of MRO's Security Advisory Council (SAC). The SAC will also meet jointly with the board's Organizational Group Oversight Committee during this meeting. Agenda materials and registration information is [here](#).

### MRO Board of Directors Meeting

June 24, 2021 | 1:00 p.m. to 4:00 p.m. Central

The MRO Board of Directors will meet next by WebEx on June 24 from 1-4pm Central. View the draft agenda and register [here](#).

### MRO Annual CMEP Virtual Conference

June 24, 2021 | 9:00 a.m. to 4:00 p.m. Central

The annual CMEP Conference is planned virtually again this year. View the draft agenda and register [here](#).

### Industry Webinar: DSM Networked Risks Workshop

June 30, 2021 | 12:00 p.m. to 3:00 p.m. Eastern

RF is hosting a Design Structure Matrix (DSM) Networked Risks Workshop on Wednesday, June 30, 2021 from 1:00 – 4:00 p.m. EST. This event will examine the interrelatedness of risks in the context of risk analysis, and we will be soliciting attendee participation to help us map risks to BPS reliability, resilience and security. Read more and register [here](#).

*In addition to the above events, MRO's NERC Standards Review Forum and Security Advisory Council Threat Forum continue to meet weekly.*

*To see more MRO meetings and events, visit our [website calendar](#).*



**Published By:**  
**MIDWEST RELIABILITY ORGANIZATION**  
380 St. Peter Street, Suite 800  
Saint Paul, MN 55102  
651-855-1760  
[www.mro.net](http://www.mro.net)

