APRIL 2022

"That is one good thing about this world...there are always sure to be more springs."

-L.M. Montgomery, Anne of Avonlea

MIDWEST RELIABILITY MATTERS

Inside This Issue

CEO MESSAGE

Silver Linings

Embracing the positives in an otherwise negative situation

I am an eternal optimist…always seeking the silver lining. Although this personality trait has served me well over the years, remaining optimistic about today's challenges is hard - really hard. The humanitarian crisis and significant rise in security threats related to the war in Eastern Europe have only added to a whole host of other twenty-first century disruptions that weigh heavily on my mind. Like many businesses, MRO is focused on moving our organization from ad hoc reactions to each disruption to a foundation of greater resilience, staying alert to what is over the horizon and building capabilities to continually evolve and manage uncertainty as the world around us changes.

The significant challenges we faced as an organization and as an industry over the past 24-plus months have taught us a lot about being flexible, adaptive and responsive to never-before-seen events. Here are some silver linings from those experiences I think we should embrace.

1: We are better prepared today than we were yesterday. Even before the war in Eastern Europe, our industry was on heightened alert to be aware of and prepare for increased cyber threats and vulnerabilities. These risks, coupled with severe weather events and the ongoing pandemic, have provided plenty of opportunity to practice crisis response and preparedness. In a span of less than two years, MRO

implemented its emergency response plan on three separate occasions. Our staff also participates regularly in NERC crisis action planning exercises and during real-life crisis action plan events. Most notably, NERC's Electricity Information Sharing and Analysis Center (E-ISAC) held its sixth grid security exercise (GridEx) in November 2021 to assist industry in preparing for a significant, coordinated cyber attack on the bulk power system. NERC recently published lessons learned and recommendations from this exercise, which include enhancing coordination, collaboration and communication amongst the electricity industry, government and cross sector partners. MRO complements the work of the E-ISAC through its Security Advisory Council Threat Forum, which meets weekly, or more often if necessary, to share information and raise awareness of new and emerging security risks within MRO's regional footprint.

2. We are more connected and capable of responding. Over the course of the pandemic and with the shift to fully virtual engagement, the importance of established connections became quite evident. I identified "connections" as one of MRO's keys to sustainable success in early 2019, and since that time our leadership team has worked to develop and foster a more connected workforce within MRO, with our ERO counterparts, and with industry stakeholders. Also in late 2018, NERC CEO Jim Robb began leading a transformation within the ERO Enterprise to be more collaborative in the work we do together to support our common vision and mission. This work was expanded in 2021 to include engagement with other regulatory agencies, policymakers and organizations that share responsibility for a reliable and secure North American bulk power system. One thing is certain – the strong relationships that have been formed and nurtured over the past three years have allowed us to quickly respond, coordinate, and collaborate in times of crisis.

3. We are continuously learning and improving. I have said before that if necessity is the mother of invention, its father must be agility and a willingness to adapt. The sudden onset of the pandemic drove a sense of urgency to find new ways to support both our staff and stakeholders. Although disruptive, the shift to being fully virtual required us to change course and develop innovative approaches to conducting daily work and accomplishing our strategic objectives. Through this experience, we learned that there are benefits to virtual work, like greater flexibility, improved accessibility, and cost savings, to name a few. Over the course of the pandemic, MRO experienced a more than double-digit increase in attendance to outreach and training events. The same health restrictions that caused us to pivot and hold all of our events in a fully virtual format also allowed us to expand our audience and reach. This experience will continue to drive innovation and process improvements in the months and years ahead as we transition to a hybrid work model where we support both virtual and in-person participation in our daily work and outreach events.

The challenges we face today are not forever. They will be replaced by new and different challenges in the future. Our collective success relies on our ability to prepare for, respond to, and learn from past struggles in pursuit of continuous improvement.

Together we can do it.

Our future is bright!

- Sara Patrick, President and CEO

Employee Spotlight

Please join us in welcoming the following individuals to the MRO Team:

Chris Pecore joined MRO's compliance team as a Senior Compliance Engineer/Auditor, CIP. His prior experience includes work at Xcel Energy in CIP substation compliance, which included conducting audits of Xcel's nuclear power plants. We look forward to the insight Chris will add to MRO's compliance team.

Rebecca Schneider joined MRO as Risk Analysis Administrator in February following a temporary assignment in the Security Department. She has several years of administrative and event planning experience that has already added significant value to MRO.

Sanja Trajkovska joined MRO as an Operations Senior Compliance Engineer following twelve years of industry experience, including technical lead and protection and control design engineer at Ulteig. Since joining MRO in January, she has already proven to be a valuable asset to the compliance team.

Please join us in celebrating the following staff retirements:

Jim Morales joined MRO in 2011 as a member of the compliance team, where he has generously shared his experience and expertise in roles as Audit Team Lead, conference presenter, and mentor. Jim has 35 years of industry experience that began after his service in the U.S. Navy on the USS Carl Vinson, Before joining MRO, Jim worked at NSP's Prairie Island Nuclear Plant as a Nuclear Plant Equipment and Reactor Operator before moving to NSP's control room in Minneapolis where he was a Control Area Operator, Transmission Operator, Network Reliability Lead, and Control Center Training Coordinator.

John Seidel has been with our organization and its predecessors for over 20 years, and was involved in the creation of MRO. His nearly 40-year career in our industry began in Chicago, where he was a planning and operations engineer for 15 years with Commonwealth Edison before transitioning to MAPPCOR in 1999. There he managed tariff administration and congestion management policies, and performed planning studies for what would eventually become the original MRO footprint. He has held several positions at MRO, most recently as Principal Technical Advisor responsible for leading the development of MRO's Regional Risk Assessment. He's contributed to countless event analyses, reliability assessments, and power system initiatives during his time at MRO, and has served on several NERC and industry committees and task forces throughout his tenure.

Russ Mountjoy joined MRO in 2007 and has held key roles in each of MRO's technical departments during his career. Russ was one of MRO's original auditors and became the first manager of MRO's compliance department. He has led MRO's Registration, Certification, and Standards efforts for a number of years and most recently joined the Reliability Analysis team, where he has been instrumental in establishing MRO's Generator Winterization Program. He also served as an MRO representatives on the FERC Cold Weather Inquiry Team.

The depth and breadth of knowledge, experience and expertise these gentlemen have shared within MRO and the ERO Enterprise is invaluable and we wish them the very best in retirement.

MRO is hiring! To apply, visit the Careers Page on our website or visit us on LinkedIn.

COMPLIANCE MONITORING AND ENFORCEMENT PROGRAM

Compliance Monitoring and Enforcement Program Update

Key Issues in Compliance, Risk Assessment and Mitigation, and Enforcement

Compliance Oversight Plans

A Compliance Oversight Plan (COP) is an entity-specific oversight strategy that begins with an assessment of the entity's inherent risk, existing controls, and prior performance. This process includes a detailed review of the entity's registration, compliance history, system performance and event history, and other risk factors. The resulting COP identifies what reliability standards are the focus for future compliance monitoring activities based on the entity's risk. The COP also identifies the appropriate interval for MRO's monitoring activities and the type of tools that should be expected during oversight. MRO currently has completed 100 percent of the COP's for Transmission Operators, Balancing Authorities, and Reliability Coordinators, where MRO is the Compliance Enforcement Authority (CEA) or the Lead Regional Entity. MRO has 15 COPs scheduled to be developed in 2022. MRO continues to innovate the COP process and is working on a streamlined process for low-inherent risk entities and is also developing tools for analyzing COPs across multiple organizations to identify trends and develop outreach opportunities, which will be utilized annually.

2022 Compliance Audit Status

MRO completes periodic Compliance Audits to assess registered entities' compliance with the NERC Reliability Standards. MRO staff has completed three of the thirteen Compliance Audits scheduled for 2022. MRO provides resources and participates in coordinated oversight audits led by other Regional Entities and is scheduled to participate or observe in five coordinated oversight audits led by another region. MRO also participated in one coordinated oversight Spot Check led by another Regional Entity. Coordinated oversight is a joint engagement with other regions for ERO approved multi-regional registered entities. Coordinated oversight Compliance Audits allow for more efficient monitoring activities for the affected registered entities. MRO also leverages these engagements to identify and share best practices with the other Regional Entities.

MRO continued to perform all Compliance Audits remotely through the first quarter of 2022. When necessary, due to COVID-19, an exception to the Rules of Procedure three-year onsite requirement has been filed with NERC. MRO is working with the ERO Enterprise to develop strategies for resuming onsite audits in a safe, effective, and efficient manner.

2022 Self-Certifications

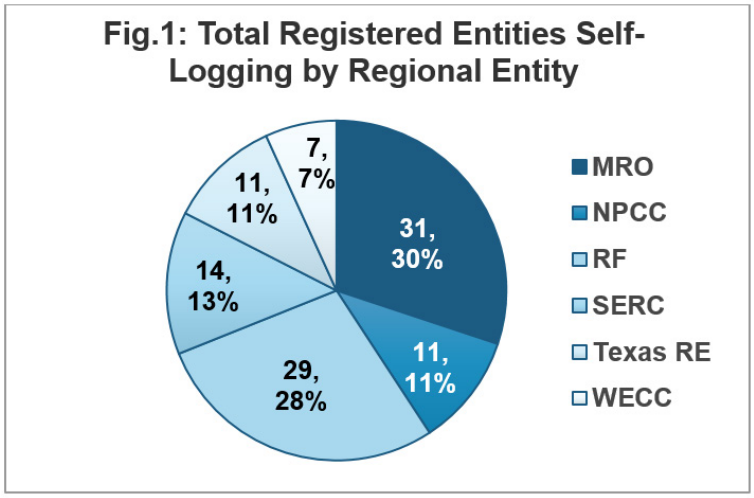
In between scheduled Compliance Audits, registered entities complete Self-Certifications of NERC Reliability Standards. MRO has revised the Self-Certification scoping process and implemented a guided Self-Certification process. The risks identified in MRO's Regional Risk Assessment and the ERO Enterprise CMEP Implementation Plan are the two primary considerations for guided Self-Certification scoping. The advantage of using Self-Certifications is that it allows MRO to address continent-wide risks and region-wide risks throughout MRO's footprint through a single process at a faster interval than Compliance Audits. MRO's Self-Certification schedule is available on its website.

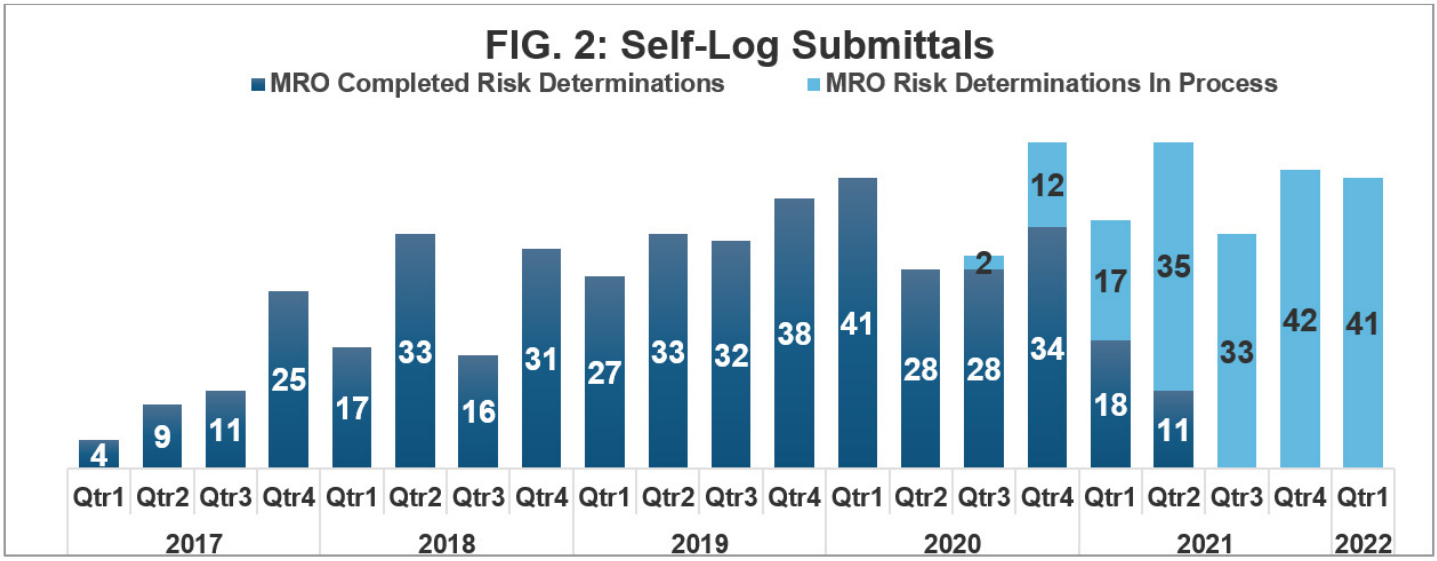
Highly Effective Reliability Organizations® (HEROs) Update

The MRO Risk Assessment and Mitigation (RAM) Department continues to monitor and respond to questions submitted to heros@mro.net. This feedback tool is widely used by MRO registered entities and serves as a great mechanism for fielding compliance-related questions. This email address has received more than 400 questions since implementation in November of 2016. Over the last quarter, MRO received 13 HEROs questions with an average response time of 12 days. This average is significantly better than the 30-day response goal.

Risk Determinations Associated with Self-Logged Noncompliances (Figure 1 and Figure 2)

Figure 1: Total Registered Entities Self-Logging by Regional Entity, shows that as of March 31, 2022, there are 31 MRO registered entities participating in the Self-Logging program, which accounts for 30 percent of all ERO Self-Logging participants. Self-Logged instances of noncompliance submitted by these participants are monitored separately as the program is designed to quickly resolve minimal risk issues that are self-identified by entities. These issues are presumed minimal risk Compliance Exceptions (CE); however, MRO has the discretion to elevate the disposition based on the RAM risk determination analysis. MRO is continually evaluating its process and outreach to improve processing efficiencies and validation of minimal risk noncompliance. Figure 2: Self-Log Submittals, illustrates Self-Logged instances of noncompliance by submittal dates. Please note submittal dates are not the start of potential noncompliance or when MRO completed its risk determination analysis.



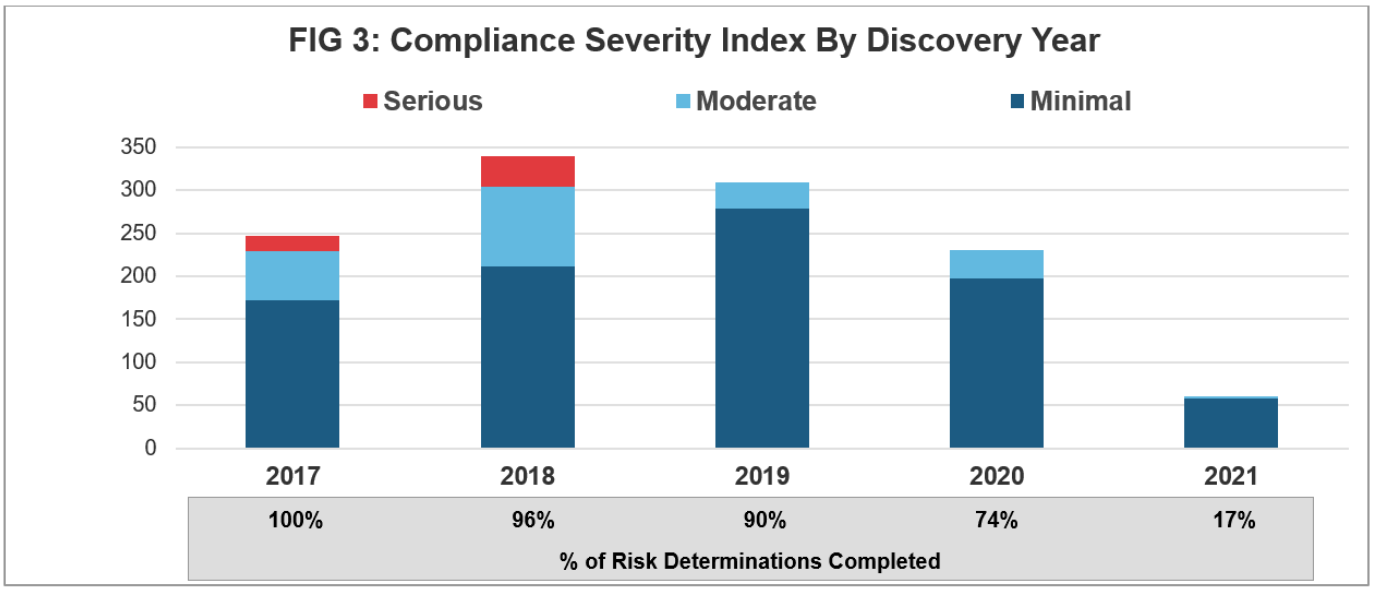


Risk Assessment and Mitigation Trends

The following charts and statistics reflect all historic noncompliances in the expanded MRO region.

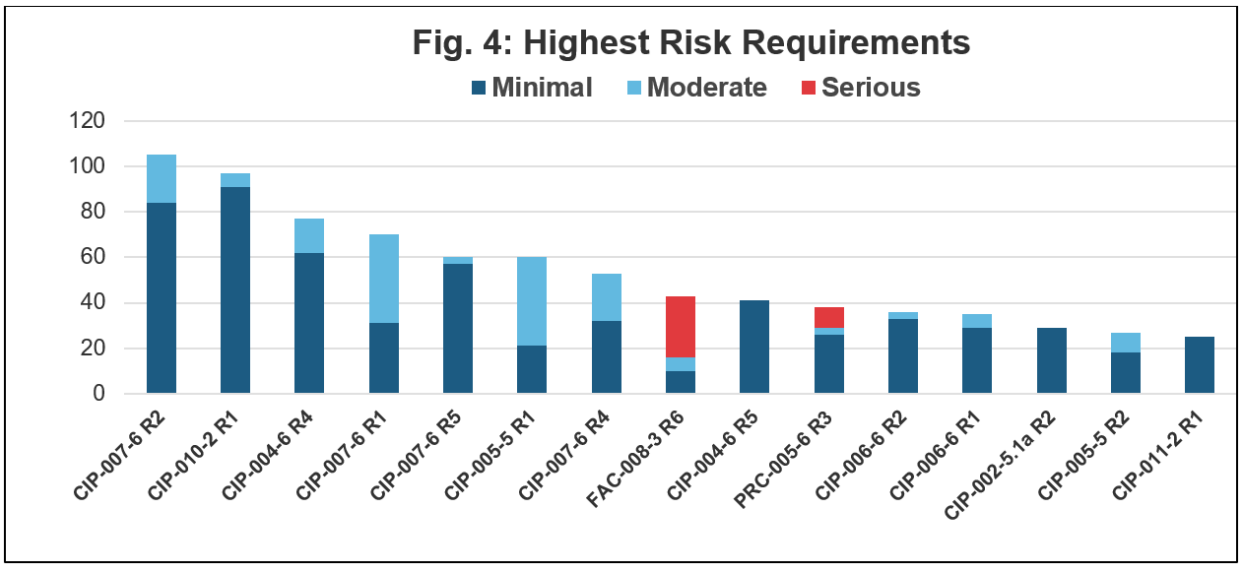
Compliance Severity Index (Figure 3)

MRO staff use the Compliance Severity Index (CSI), shown in Figure 3, to evaluate progress toward a key reliability goal of less severe violations. The CSI represents the total risk that instances of noncompliance bring to the reliability or security of the bulk power system in the MRO region. The CSI is calculated using the risk determination and Discovery Method for each noncompliance. MRO has seen a notable decrease in the risk of issues of noncompliance over the past decade due to an overall improvement in the culture of compliance. Registered entities are self-identifying issues of noncompliance in a timely manner prior to issues presenting a greater risk to reliability.



Highest Risk Noncompliances (Figure 4)

Figure 4 provides the 15 highest risk requirements, from January 1, 2017 to March 31, 2022, that have a history of issues of noncompliance, based on the CSI. Higher risk violations are associated with cyber and physical security standards, accurate facility ratings, and timely maintenance of protection systems.

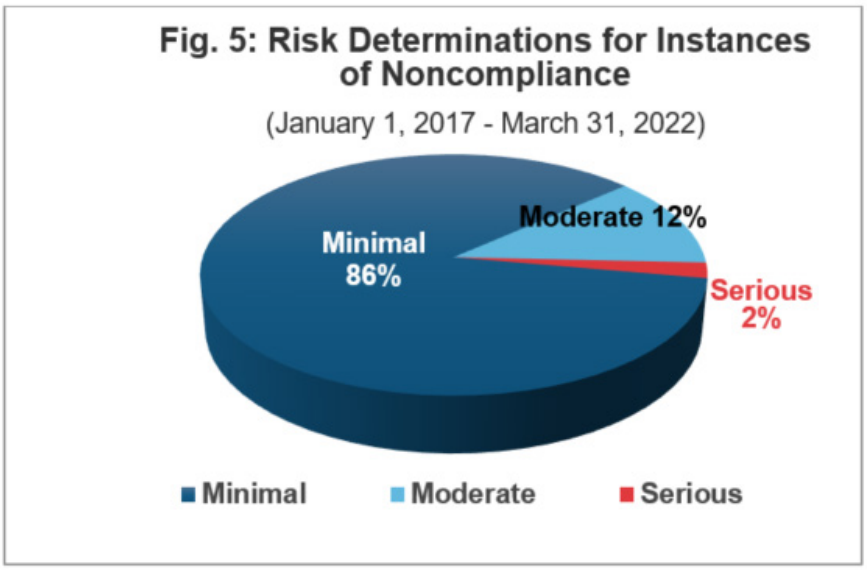


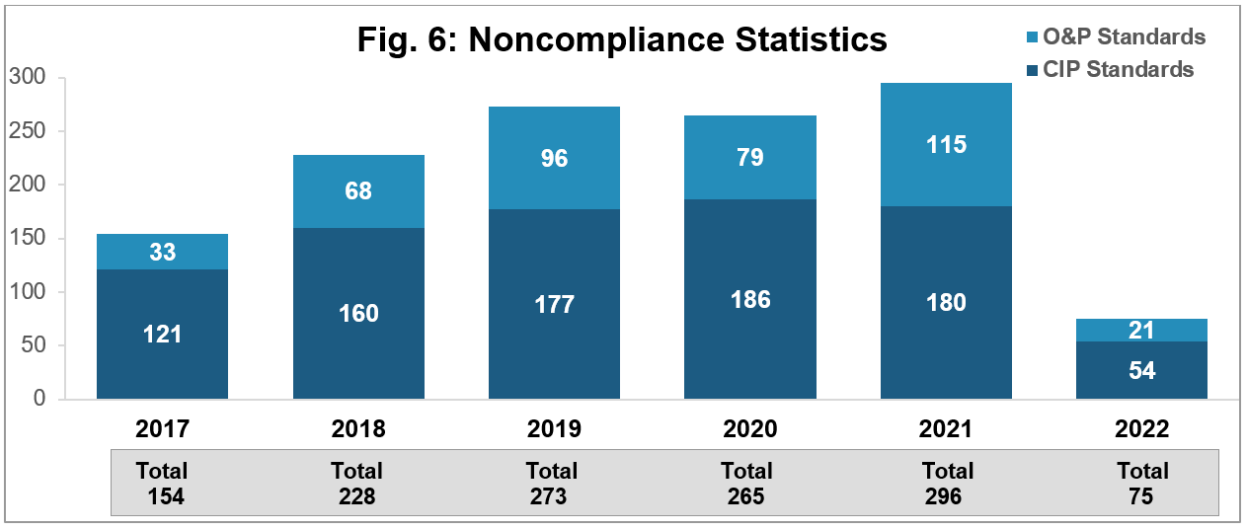
Description of the Top Five Highest Risk Requirements (Figure 4)

- CIP-007-6 R2: Requires a patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. A high volume monthly requirement in which even the most mature security programs will have an occasional non-compliance.
- CIP-010-2 R1: Requires current baseline configurations for applicable Cyber Assets.
- CIP-004-6 R4: Implement access management programs which authorize access to applicable BES Cyber Systems.
- CIP-007-6 R1: Intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and services and physical I/O ports.
- CIP-007-6 R5: Has a method(s) to enforce authentication of interactive user access to applicable Cyber Assets.

Risk Determinations of all Instances of Noncompliance (Figure 5)

Ninety-four percent of all instances of noncompliance from January 1, 2017 to March 31, 2022, were determined to be minimal risk. There is a correlation between the increasing percentage of issues of noncompliance being minimal risk (Figure 5) and the increasing percentage of self-reported issues of noncompliance (Figure 7). Entities are identifying noncompliance before the issues become more impactful to the reliability and security of the bulk power system.





Noncompliance Trends and Statistics

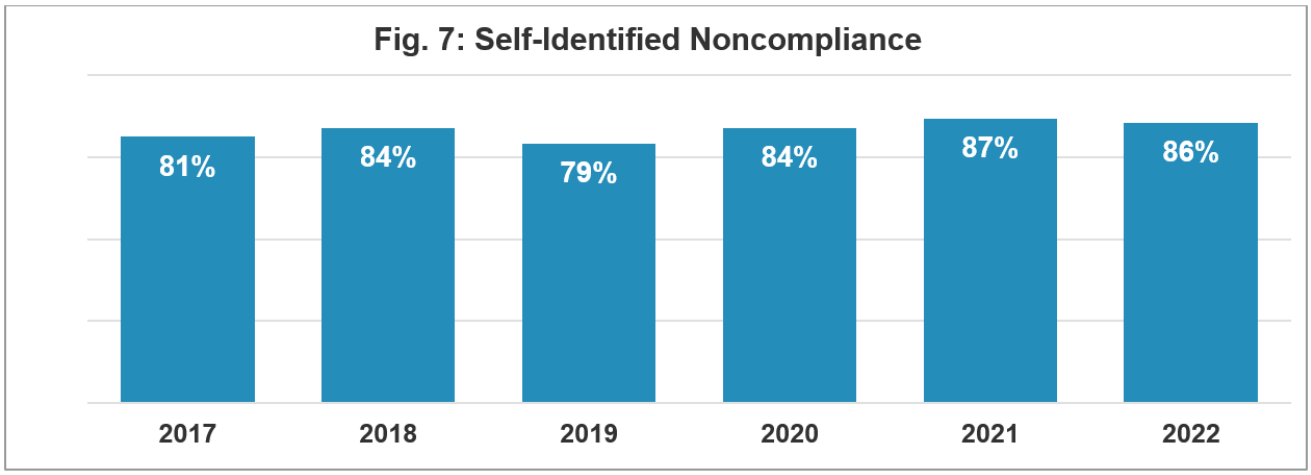
Breakdown of Critical Infrastructure Protection (CIP) vs. Non-CIP Possible Noncompliance (Figure 6)

The noncompliance statistics and trends in Figure 6 on page 9 are annually discovered and reported to NERC from January 1, 2017 to March 31, 2022.

Registered Entity Responsibility (Figures 7 and 8)

MRO staff analyzes how often registered entities self-identify and accept responsibility for noncompliance. These trends are indicators of the commitment among registered entities in the region to perform self-assessments of their compliance with the reliability standards. The high percentages, reflected in Figure 7 and Figure 8, demonstrate a strong governance and compliance culture of registered entities in the MRO region, as well as registered entities' willingness to accept, and learn from, discovered issues of noncompliance in order to prevent future noncompliance with NERC Reliability Standards.

Figure 7 reflects issues of self-identified noncompliance that MRO processed from January 1, 2017 to March 31, 2022. Figure 8 shows the percentage of time that registered entities have accepted responsibility for noncompliance submitted to NERC or another applicable Regulatory Authority from January 1, 2017 through March 31, 2022.



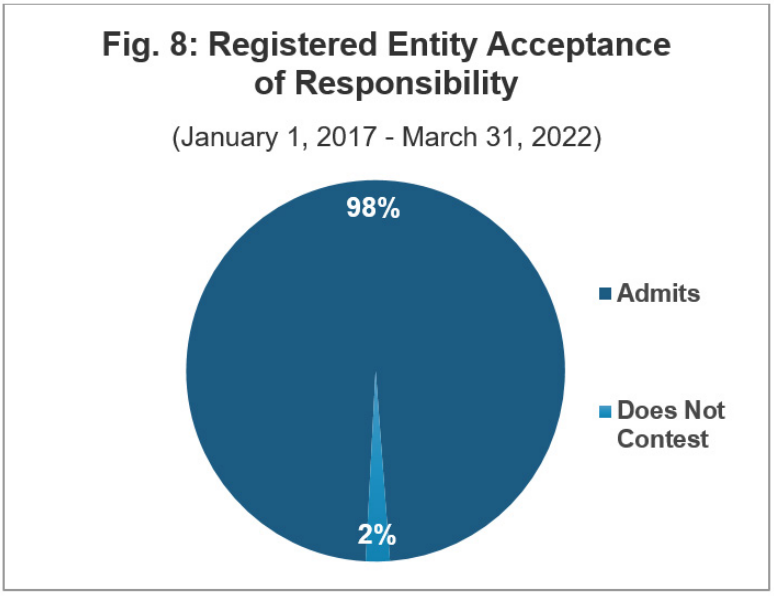


Figure 9: Discovery Method

Discovery Method Detail	2017	2018	2019	2020	2021	2022	Sub Total	(-less) Dismissed	Total
Compliance Audit	26	33	47	40	18	1	165	19	146
Compliance Investigation	0	0	0	0	0	0	0	0	0
Data Submittal	0	0	0	0	0	0	0	0	0
Self-Certification	2	23	10	5	16	9	65	11	54
Self-Log	49	97	131	145	156	41	619	8	611
Self-Report	75	75	85	75	106	24	440	25	415
Spot Check	2	0	0	0	0	0	2	0	2
Totals	**154**	**228**	**273**	**265**	**296**	**75**	**1291**	**63**	**1228**

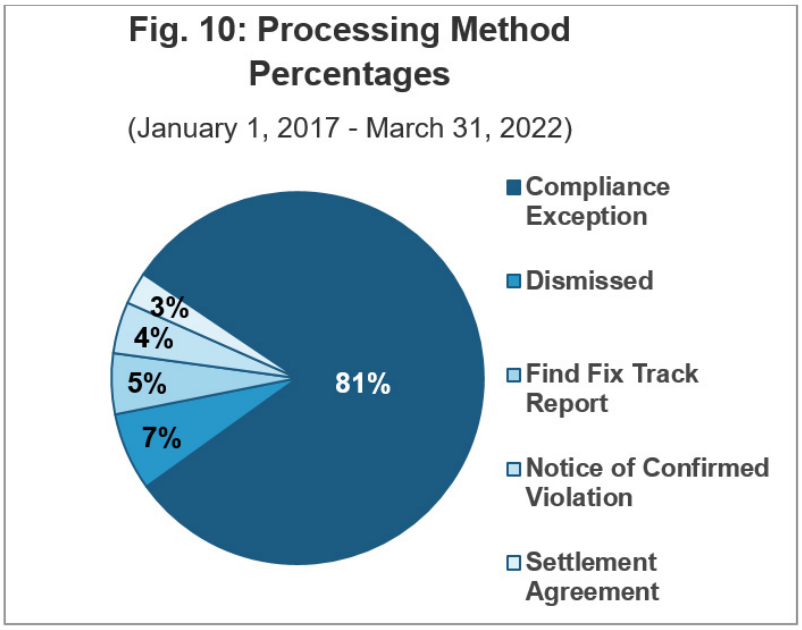
Discovery Method Detail (January 1, 2017 through March 31, 2022) (Figure 9)

In Figure 9, the numbers reflect all noncompliances in the MRO region that were reported to NERC or other applicable Regulatory Authority.

Noncompliance Processing (Figure 10)

MRO staff analyzes trends in the status of noncompliance processing by compiling all available processing methods, the average age of open noncompliances, and the closure percentage of noncompliances for each year. This analysis indicates progress towards simpler, more expedited processing due to the increased use of CEs to process minimal risk noncompliance.

Figure 10 includes issues of noncompliance for entities that were registered in the MRO region during the specified time period.

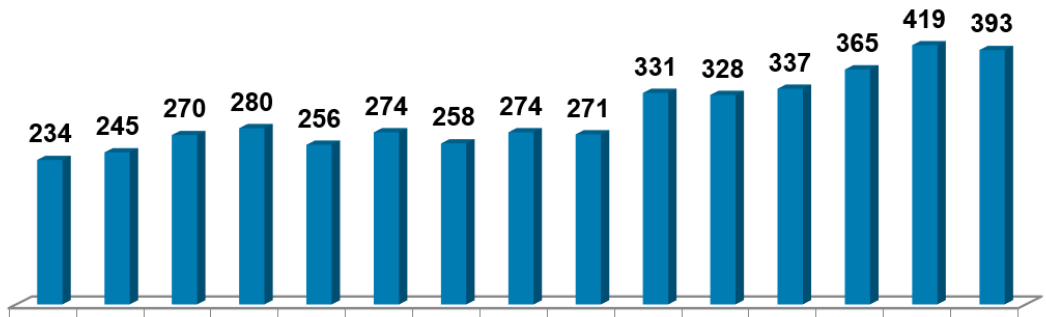


Noncompliance Processing Time (Figures 11 and 12)

Figure 11 illustrates the trend of the average age for open noncompliances in MRO's inventory. The average processing for these open noncompliances is calculated by using the date reported to MRO until the last day of the noted quarter or specific date indicated and taking the average of the calculated days.

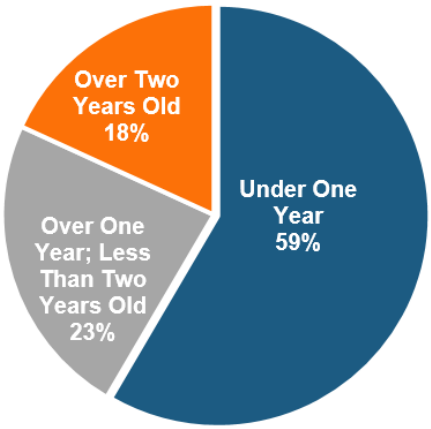
Figure 12 illustrates the aging time for all open instances of noncompliance reported to MRO and applicable government authority.

Fig. 11: Quarterly Aging Average for Noncompliance Reported to NERC and Currently in Process



	3rd Qtr 2018	4th Qtr 2018	1st Qtr 2019	2nd Qtr 2019	3rd Qtr 2019	4th Qtr 2019	1st Qtr 2020	2nd Qtr 2020	3rd Qtr 2020	4th Qtr 2020	1st Qtr 2021	as of 8/31/ 2021	as of 9/30/ 2021	as of 12/31 /2021	as 3/31/ 2022
Average # of Days for Open Cases	234	245	270	280	256	274	258	274	271	331	328	337	365	419	393

Figure 12: Age of Open Noncompliance in MRO Inventory



For questions on this report, please contact the following individuals:

Compliance Monitoring: Jeff Norman at 651-855-1703 or jeff.norman@mro.net.

Risk Assessment & Mitigation: William Steiner at 651-855-1718 or william.steiner@mro.net.

Enforcement: Tasha Ward at 651-256-5188 or tasha.ward@mro.net.

Align and SEL Project Update

Release 3

Performance optimization efforts for Release 3, as outlined in the January edition of the Align Newsletter, are completed. MRO's R3 adoption approach is listed below along with the following activities that were identified as part of the modifications for Release 3:

- Redesigned Periodic Data Submittal and Self-Certification in the assignment area - instructions will be sent out to Primary Compliance Contact's by the end of April.
- Refactored database queries for dashboards and reporting capability.
- Vendor review of Release 3 audit design to ensure optimal performance.
- Additional performance testing performed by a third party.

Region	Adoption Approach
MRO	Will start in April 2022 with the first notification for Q3 coordinated oversight audit; will complete one audit end-to-end, then review processes for lessons learned.

Release 4

The Align Steering Committee approved the scope of Release 4, which will include additional required features for audit and scheduling, inherent risk assessments (IRAs), and compliance oversight planning (COPs). Release 4 will have two production deployments: R4.0 will deploy in June with enhanced audit and scheduling functions, and R4.5 will deploy in October with IRAs and COPs. This approach will enable valuable features sooner and allow for focused training and adoption plans.

Canadian Jurisdictions' Use of Align

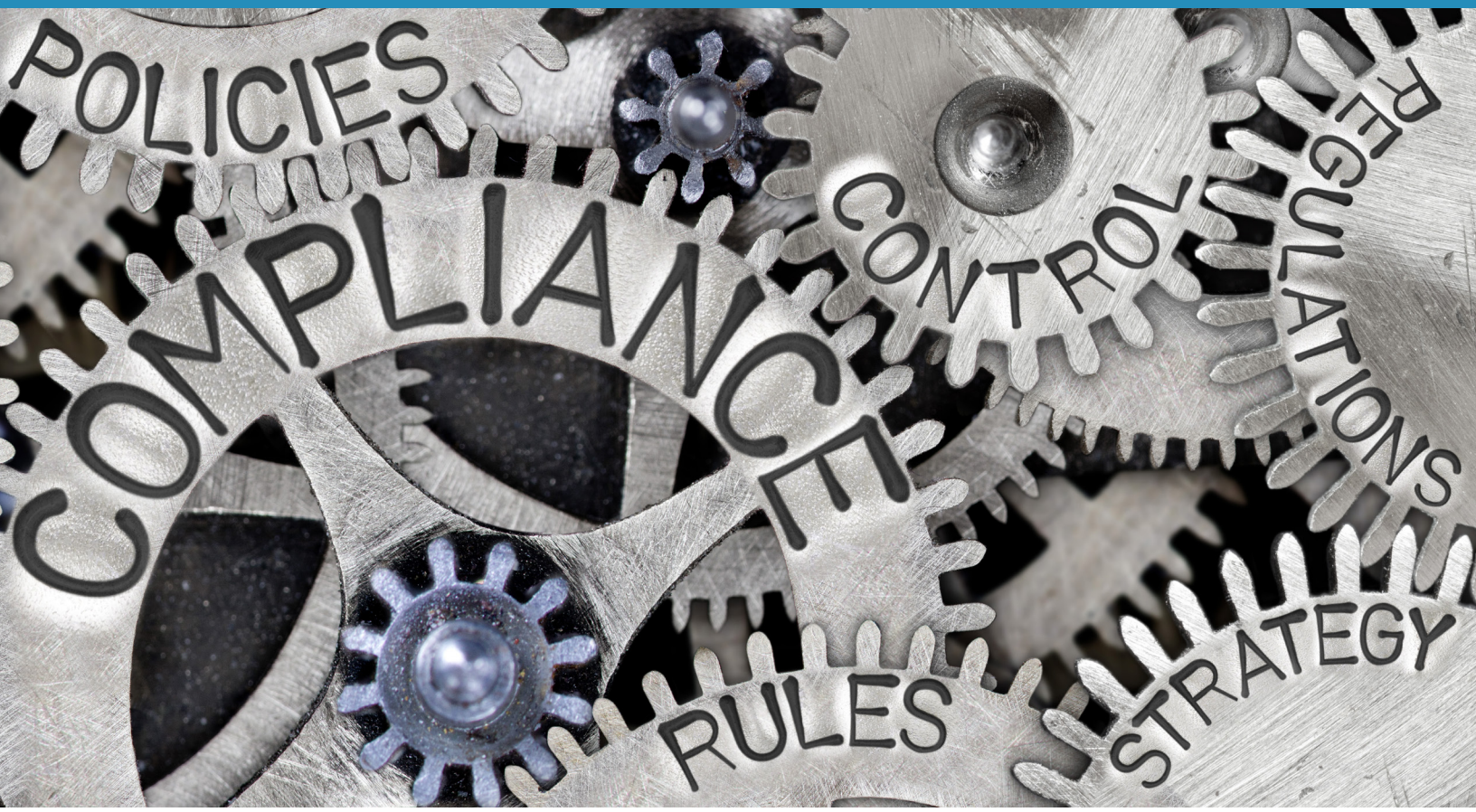
The Align project team continues to work with those Regional Entities that support Canadian regulators—MRO, NPCC, and WECC—to create project plans and activities in support of using Align. These activities include determining detailed requirements by province, importing provincial standards data into Align, and defining the appropriate user roles. The requirements definition work is completed. The project team will analyze the requirements to determine a schedule for implementation. This schedule will be shared with the Regional Entity Change Agents as soon as it's available and in the May Align newsletter.

If you experience any technical issues with Align or the ERO SEL, please submit a NERC help desk ticket here.

- Desirée Sawyer and Marissa Falco, MRO Align Change Agents

The most recent NERC Standards, Compliance and Enforcement Bulletin can be found here.

REGISTRATION, CERTIFICATION AND STANDARDS



Annual Certification Reminder

All NERC registered entities that are Balancing Authorities (BAs), Reliability Coordinators (RCs), and Transmission Operators (TOPs) are required to be certified to perform these respective functions because they are deemed crucial to reliability of the bulk power system. Certification verifies that each of these registered entities have the tools, trained staff, processes, procedures, and the necessary cyber and physical controls in place to meet the requirements of applicable NERC Reliability Standards. Certification is not a periodic activity. Once certified, entities are not subject to periodic certification activities as long as there are no material changes to an entity's scope of operations.

All BAs, RCs, and TOPs experiencing a material change to operations are asked to notify MRO certification staff of those changes, which may require a certification review by MRO. Reviews are a condensed version of the initial certification, focused solely on the change affecting the entity's real-time operations. An example of events that may trigger a certification review could be any of the following:

- Changes to the registered entity's footprint
- Relocation of the entity's Control Center
- Modification of the entity's Energy Management System (EMS)

Entities experiencing these changes are asked to complete the MRO Certification Preliminary Questionnaire. The

questionnaire will provide MRO staff a greater understanding of the scope of the change and its impact. After review of the questionnaire, MRO may:

- Ask for further details, which may or may not necessitate scheduling a review;
- Schedule a review;
- Consider a lesser activity;
- Consider the event to be closed, requiring no further action.

Even though the NERC Reliability Standards are a large component of the certification review process, certifications and certification reviews are not compliance monitoring activities, as the review is proactive. Certification reviews are focused on determining if all the necessary steps are in place to prepare for the change impacting operations. Areas of concern identified during the review provides the opportunity for the registered entity to make corrections with no compliance implications. As part of the certification review, registered entities may also receive non-binding recommendations for consideration.

Registered entities have discovered that certification reviews provide one more level of assurance that the changes will not impact the ability to maintain reliable operations. MRO's Certification Review Team is comprised of experts who have worked with other registered entities experiencing similar changes to their operations, and are familiar with obstacles or issues that might result from those changes.

If you are an MRO registered entity that is planning on a change in the next 12 months, or you have any questions related to certifications, please contact MRO at certification@mro.net.

- Russ Mountjoy, Principal Reliability Specialist

EOP-004-4 Event Reporting

Overseeing reliability of the North American bulk power system has resulted in a heightened focus on the effects of human error. As such, MRO is taking an in-depth look at Reliability Standard EOP-004-4 (Event Reporting) data submissions, and the meaning of the phrase "contrary to design" and the role it plays in both EOP-004-4 oversight and the ERO Event Analysis Program (EAP). The standard and the EAP have been aligned since the development of an earlier version of the standard (EOP-004-2), when the Standard Drafting Team (SDT) coordinated with the NERC Event Analysis Subcommittee (EAS) to develop a comprehensive list of event types to be reported.

Within the comprehensive list in EOP-004-4 Attachment 1: Reportable Events, is the event type "transmission loss," which is applicable to Transmission Operators (TOPs). The threshold for transmission loss is identified as: unexpected loss within its area, contrary to design, of three or more Bulk Electric System (BES) Elements caused by a common disturbance (excluding successful automatic reclosing). In the Standard Project 2015-08 Consideration of Comments and Responses, the SDT acknowledges the link between the EOP-004 standard and Event Analysis. In addition to confirming that the EOP-004-4 Transmission Loss event type in Attachment 1 is closely aligned with or linked to the EAP, the SDT further suggests that one could look to the NERC (EAP) website for event examples, specifically the Addendum for Determining Event Category.

Although not in NERC's Glossary of Terms, guidance exists for the term "contrary to design" within the EAP

Addendum for Determining Event Category. Contrary to design does not apply to each individual element, but rather to the three elements as a whole. If a scheme is designed to trip three elements for a single fault, that is "as designed." If a single line fault results in the faulted line tripping along with two other lines misoperating and tripping, which is three elements outaged due to a common disturbance, or "contrary to design." The example would be a qualified event. This definition is under the breakdown of EAP event category 1.a.i, which is identified as "an unexpected outage, contrary to design, of three or more BES Facilities caused by a common disturbance."

Human error is specifically called out in the EAP Addendum for Determining Event Category as part of the section "Contrary to Design, Unintended." The ERO Enterprise views human error as an unintended and unexpected cause of an event and considers it to fall within the EAP language "contrary to design." Human error that initiates the unintended outage of three or more BES facilities, even though the protection schemes for those facilities operated correctly, is not the "designed" intent of any protection scheme. A disturbance or outage of any type should never be considered the intended outcome of maintenance or testing work. Human error that causes three or more BES facilities to be outaged requires investigation and corrective actions in order to prevent reoccurrence and also should be shared with industry to avert similar events elsewhere on the system.

Compliance with EOP-004-4 is mandatory, while participation in the EAP is voluntary. The standard's purpose provides situational awareness and the necessary preparation to mitigate current and further events, while the EAP provides root causes analysis, focuses on capturing trends, and allows sharing valuable lessons learned with industry. Although it may seem burdensome to report twice for one event (once for EOP-004 and once for EAP), each report has its own separate purpose/intent. Because the SDT acknowledged the EAP to be closely aligned to EOP-004-4 and further references the use of EAP documentation to help guide reporting for compliance, MRO will be evaluating EOP-004-4 Transmission Loss events to include those caused by human error, as they are specifically part of unintended contrary to design.

Consistent reporting of event information to both the EOP-004-4 and EAP processes support the ERO's efforts to assess risk to the BES. MRO advises registered entities to contact staff if there is a question about whether an event report should be submitted per the EOP-004-4 reporting process and/or the EAP process. *Example: Cat 1.a event of 3 or more occurs contrary to design and it includes 2 BES lines and one BES generator. But the generator is off line at the time of the event due to economic dispatch yet considered as available by the RC (it's not forced out or out for maintenance). The entity is not sure if that generator should be counted or excluded. The entity contacts MRO, MRO then assigns staff (internal SMEs) to assist the entity in the review and determine as to whether an EA report and/or EOP-004 notification is warranted*.

All EOP-004 and OE-417 notifications/forms, should be sent to systemawareness@nerc.net (which follows the ERO Periodic Data Submittal Schedule) as well as events@mro.net. EAP brief reports should be sent to events@mro.net. MRO staff will work with entities to upload larger event reports or ones that contain Critical Energy Infrastructure Information data to MRO's confidential FTP site for security. In addition, MRO suggests that entities utilize the MRO events email address to communicate why and/or how a specific event is deemed not applicable to EOP-004-4 or EAP reporting. Questions regarding events and reporting can also be directed to heros@mro.net.

- Summer Stephens, Senior O&P Risk Assessment and Mitigation Specialist

Lake Leander, Britt, MN 4:30 a.m., November 4, 2021 (credit: Richard Samec)

The Magic Surrounding Reliabiity Standard EOP-010-1

The solar phenomena leading to mitigation of the effects of geomagnetic disturbance events can also lead to once-in-a-lifetime magical experiences!

On a cold, clear November night in 1984, as part of a group of students returning home from a Chuck Mangione concert in Duluth, Minnesota, the skies opened up to provide the most magnificent display of the aurora borealis I had ever seen. For the 37 years to follow, I imagined whether I might see another display as breathtaking as the one I witnessed that night.

As monitoring technology has evolved over time, we are finding space weather information easily accessible at our fingertips. Most informative are the Kp threshold alerts, where Kp is an indicator of disturbances in the Earth's magnetic field leading to displays of the aurora borealis, especially at higher altitudes.

Fortunately, the sky is free of light pollution at my northern Minnesota lake cabin. Upon subscribing to the *SWPC Product Subscription Service* real-time Kp Index email alerts some years back, I've been led to make numerous trips north, promoted by the alerts and my own sense of hope, fueled by optimism. However, it seemed that thickening

clouds, too much moonlight, or a no-show in the actual Kp index always ruined my chances of seeing the aurora. Or, when the aurora was actually visible, I wasn't able to drop everything and head north. This led to many years, even decades, of auroral "swings-and-misses."

Then, in early November 2021, the SWPC and social media interest groups lit up when an impending geomagnetic sudden impulse (a change the magnetic field following a solar flare) was expected to occur in the hours to come. At that time, the SWPC elevated its forecast to a potential G3 (strong) geomagnetic storm.

Drop everything. Grab camera. Drive to cabin.

Upon my 11 p.m. arrival to the dark wilderness, SWPC emailed a notification that Kp=6 was reached. I quickly made my way to the south side of the lake where there is an open beach looking north, and I set up my camera. While the aurora was visible for a short time, the intensity was already declining, and soon some thin clouds obscured the sky.

Back at the cabin, I awoke at 3:50 a.m. the morning of November 4 and checked my email only to see page after page of notifications from SWPC with the latest notification indicating Kp=7 had been reached! I stumbled to the back door in my pajamas and looked outside, and was greeted by visible aurora movement and pillars straight overhead. I knew that any auroral displays that are visible overhead in Minnesota means that *The Big One* is underway! And, this was indeed THE BIG ONE!

Not wasting even a moment, I threw on layers of warm clothes over my pajamas, grabbed my camera and tripod, and barreled out to my truck - making my way to the beach, shivering with excitement.

Upon arrival, what unfolded before me was an absolutely magical sky, starlit and illuminated 180 degrees east to west, and from the horizon upwards to the sky straight above me. Dancing ribbons and columns of green, gold, blue, pink, and magenta moved overhead for the next 90 minutes, all reflected on the calm surface of the lake. I captured 92 time-exposed photographs, each of which is incredible and unique. I am still so grateful for having the forecasted and real-time data to know exactly when to show up!

In 1984, I could not have imagined that this magnificent phenomena could put reliable electricity at risk. Fast forward almost four decades, working for an organization charged with reliable operations of the North American bulk power system, I feel reaffirmed by the power of nature.

NERC's Reliability Standard EOP-010-1 exists to mitigate the effects of a Geomagnetic Disturbance Event on the power grid. I have been fortunate enough to witness the magical qualities of such an event first hand.

Albert Einstein said it best: "Look deep into nature, and you will understand everything better."

- Rich Samec, Principal Compliance Engineer

National Oceanic and Atmospheric Administration (noaa.gov)

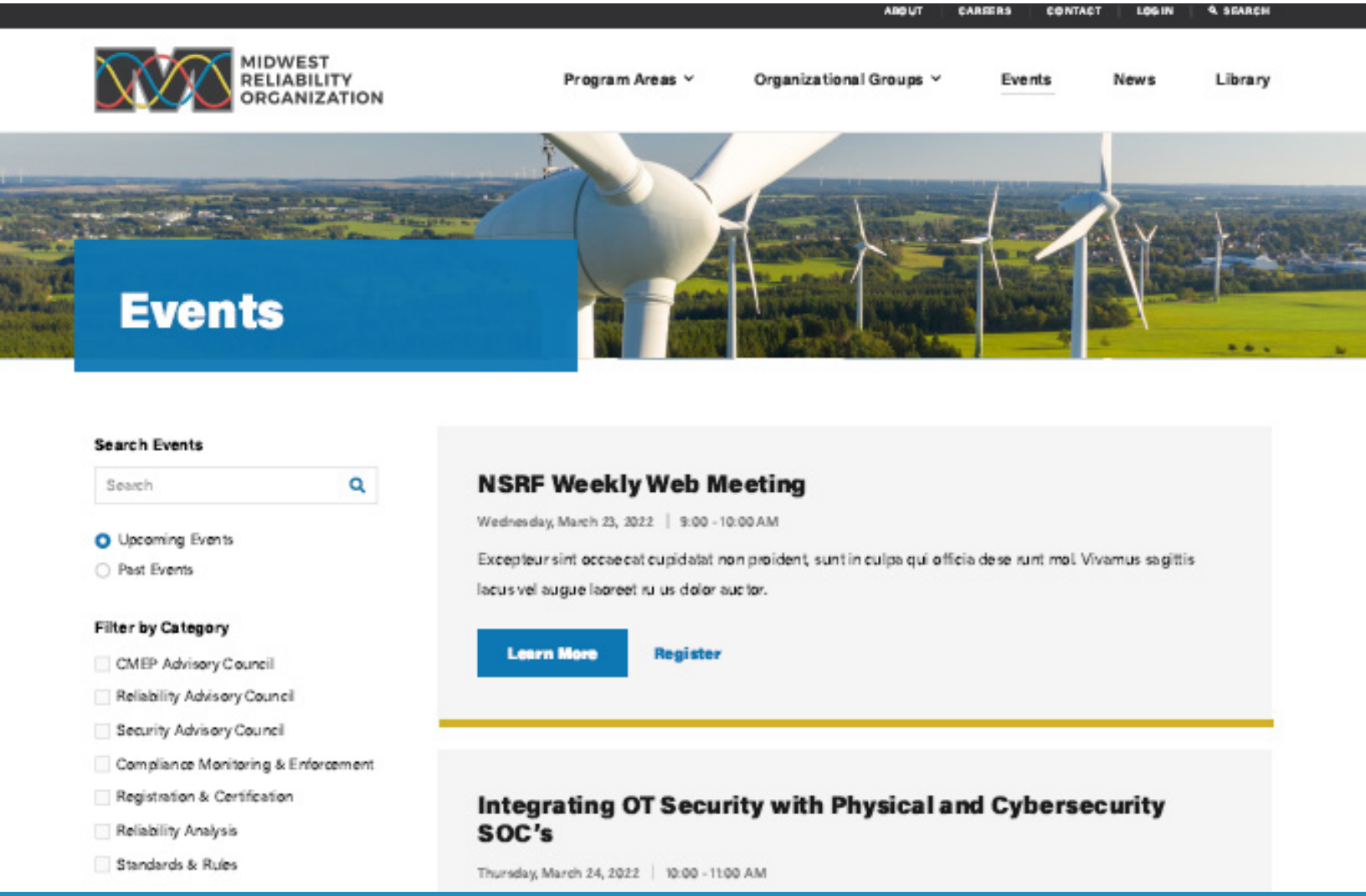
SWPC Product Subscription Service Examples:

Geomagnetic Sudden Impulse Alert:

```
Space Weather Message Code: WARSUD
Serial Number: 185
Issue Time: 2021 Nov 03 1949 UTC

WARNING: Geomagnetic Sudden Impulse expected
Valid From: 2021 Nov 04 2005 UTC
Valid To: 2021 Nov 04 2105 UTC
IP Shock Passage Observed: 2021 Nov 04 1942 UTC
```

K-Index Alert:

```
Space Weather Message Code: ALTK07
Serial Number: 119
Issue Time: 2021 Nov 04 0934 UTC

ALERT: Geomagnetic K-index of 7
Threshold Reached: 2021 Nov 04 0934 UTC
Synoptic Period: 0900-1200 UTC

Active Warning: Yes
NOAA Scale: G3 - Strong
```



NEW MRO WEBSITE COMING IN JUNE

For some time now, our stakeholders have been asking us to improve the navigation of our website and its search capabilities. In January, we polled individuals from MRO registered entities and other stakeholders that frequently use the website to seek input on the website's functionality and what opportunities exist for improvement. Since that time, a small team of MRO staff has been working with an external firm to design and develop a new site that better meets the needs of our stakeholders.

We are very excited to announce that MRO will go live with a new website this June!

Some of the website enhancements you can look forward to are:

- Structure designed around key program areas, organizational groups, industry events, news, and information
- Drop down menu items for easier navigation
- Improved search functionality and the ability to sort news and library items by category and document type
- Ability to subscribe to specific areas of interest
- Integrated social media buttons to share important information

Our goal with the new site is to provide end-users with easier access to information highlighting the important work we do to forward our vision of a highly reliable and secure North American bulk power system. Stay tuned for more!

EXTERNAL AND REGULATORY AFFAIRS

State Regulatory Outreach Initiative

The ERO Enterprise state outreach initiative is continuing to strengthen relationships between ERO Enterprise staff and other regulatory agencies, enabling the ERO to become a valued and trusted resource for federal and state regulators. Additionally, MRO continues to coordinate with neighboring regions on outreach opportunities in states located within multiple regional footprints. On December 16, 2021, MRO, ReliabilityFirst, and SERC Reliability Corporation, along with staff from NERC and the Federal Energy Regulatory Commission (FERC), presented the final report of the 2021 Cold Weather Event at the Organization of MISO States board meeting. The same group of MRO, ReliabilityFirst, and SERC Reliability Corporation subject matter experts gave this presentation at the December 17, 2021, Organization of PJM States, Inc., meeting.

On March 7 and 9, 2022, Bryan Clark, director of reliability analysis, and I, along with SERC Reliability Corporation staff met with commission and technical staff from the Missouri Public Service Commission to discuss the ERO Enterprise Long-Term Reliability Assessment and MRO's Regional Risk Assessment and how the two assessments impact Missouri and neighboring states. On March 14, 2022, Bryan Clark and I met virtually with the Iowa Public Utilities Board Commissioners and commission staff and presented a high-level overview of MRO's Regional Risk Assessment. On March 15, 2022, Bryan Clark and I discussed the same topics with the executive director and one board member from the Nebraska Power Review Board.

On April 22, 2022, Sara Patrick, President and CEO, will attend a joint meeting with the NERC Board of Trustees and NARUC's Electricity Committee. This meeting will focus on strategic reliability and security issues, including the intersection of state and federal jurisdictions. Additionally, MRO will continue to send communications and meet with state regulators to provide information on MRO and the ERO Enterprise and inform these agencies of public reports published each year highlighting the risks and challenges facing the bulk power system. These correspondences also highlight opportunities to attend educational events hosted by MRO and the ERO Enterprise.

I will also attend the Mid-American Regulatory Conference (MARC) Annual Meeting on June 19-23, 2022. MARC is an association of regulatory agencies from 14 Midwest states (Arkansas, Kansas, Illinois, Indiana, Iowa, Michigan, Minnesota, Missouri, Nebraska, North Dakota, Oklahoma, South Dakota, Texas, and Wisconsin). The annual meeting is attended by state commissioners, commission staff, and representatives of regulated industries and is open to the public. Topics on this year's agenda include *FERC Order No. 2222 Use Cases and Implementation* and *Building for the New Normal: Development of Grid Enhancement Investments and Other Technologies*. MRO will continue to send communications about MRO and ERO Enterprise public reports and conferences to state commissions and commission staff and will continue to coordinate with bordering Regional Entities on outreach opportunities in states within multiple regional footprints.

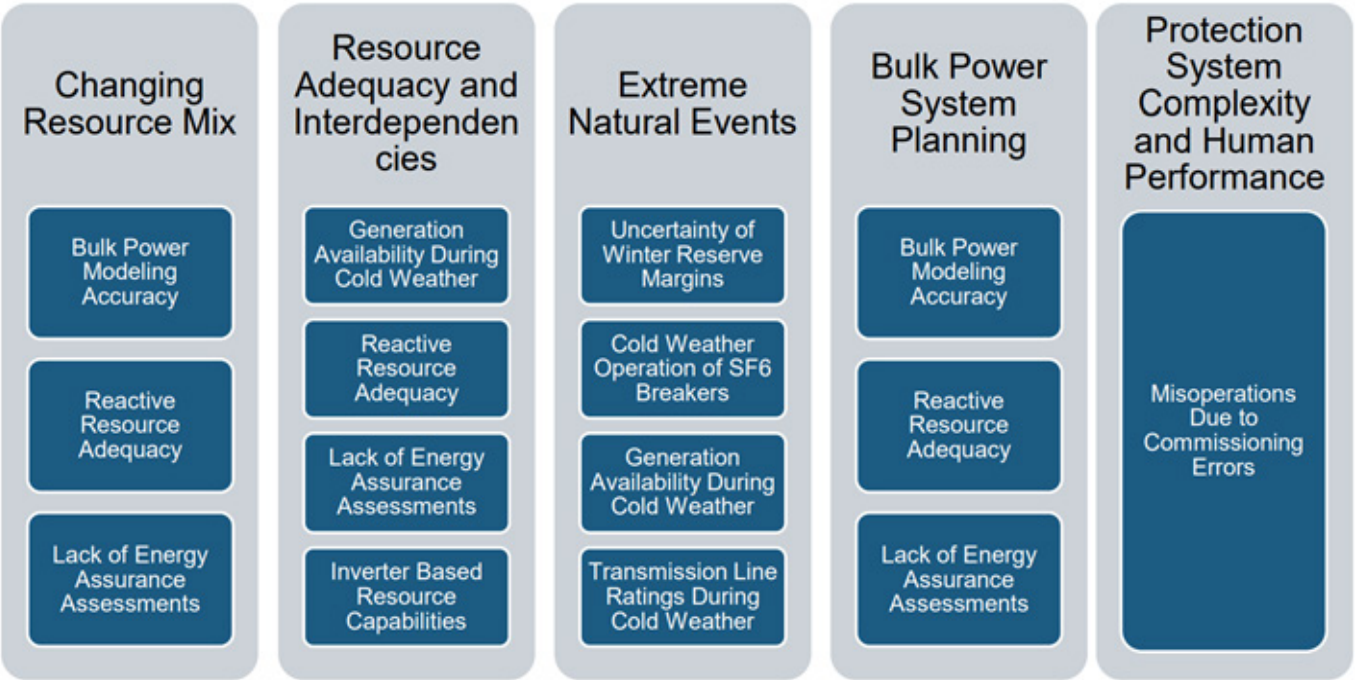
If you have any questions, do not hesitate to reach out to me at tasha.ward@mro.net.

BULK POWER SYSTEM RELIABILITY

The Need for Energy Assurance Assessments

As the bulk power system continues to be supplied with more non-synchronous resources—such as renewables, battery storage, and demand response—new ways of operating the system have created challenges related to assessing resource adequacy. The traditional method of focusing on generating capacity compared to peak load in order to determine planning reserve margins is proving to not be as reliable as in the past, specifically in extreme conditions. Because of this, energy assurance has become one of the top risks challenging bulk power system owners, users and operators across the North American continent and within the MRO region. It was identified as one of seven high risks most impactful to the MRO region as part of MRO's 2022 Regional Risk Assessment.

Figure 1 on the following page reflects the bulk power system planning risks identified in the annual risk priorities report published by NERC's Reliability Issues Steering Committee (RISC). All of these risks contribute to the broader risk of energy assurance as they impact the ability to reliably serve load or system demand. NERC's Energy Reliability Assessment Task Force (ERATF) is working on an action plan to address this issue.



Recognizing that energy assurance assessments can serve as a supplement to the traditional methods used to assess planning reserve margins, the ERATF's main focus is to analyze two parameters: 1) fuel assurance and flexibility based on the evolving resource mix, and 2) gas delivery security.

These two parameters need to be analyzed in the following time horizons:

- Operational
- Near-Term Transmission Planning
- Long-Term Transmission Planning

The ERATF is also developing a Standard Authorization Request (SAR) titled Fuel Assurance with Energy-Constrained Resources that will be submitted to the NERC Reliability and Security Technical Committee (RSTC) for endorsement and then the Standards Committee for approval in June. The group hosted a webinar on February 16 that covered the key findings from the technical paper.

MRO staff and a stakeholder representative from the region have been assigned to closely follow the activities of this group in order to support and provide input on this high risk. More information on this very important task force can be found here.

- Bryan Clark, PE, Director of Reliability Analysis

Why Timely Data Submission is Important

In order to review, assess, and meaningfully report on the reliability of the North American bulk power system, the North American Electric Reliability Corporation (NERC) and the six Regional Entities (of which MRO is one) rely on data provided by registered entities in accordance with Section 1600 of the NERC Rules of Procedure. Each Section 1600 data request specifies the data to be collected, the registered entity function(s) to which it applies, the criteria for reporting requirements, and how and when the data will be collected. The Rules of Procedure give MRO the authority to request the data and information needed to meet its obligations under section 215 of the Federal Power Act. Of particular importance to NERC and MRO are the data collected from registered entities that meet reporting requirements for the following:

- Generation, collected under the Generating Availability Data System (GADS & GADS Wind)
- Transmission, collected under the Transmission Availability Data System (TADS)
- Protection system operations, collected under the Misoperation Information Data Analysis System (MIDAS)

Data collected through these requests is analyzed regularly, resulting in key findings and recommendations that serve as technical input to NERC, MRO, and industry reliability activities. Notably, the findings are published in NERC's annual State of Reliability Report and MRO's seasonal Summer Regional Assessment and Winter Regional Assessment, as well as various webinars, newsletters, and other publications. Accuracy and timeliness in reporting the data is critical to the development of these reports.

Collection of data begins with the annual Section 1600 Reporting Confirmation. All NERC registered Transmission Owners (TOs), Generator Owners (GOs) and Distribution Providers (DPs) are required to annually provide NERC with information about whether they meet the reporting criteria for Section 1600 data requests. Each registered entity is required to complete the Section 1600 Reporting Confirmation in the NERC ERO Portal by January 15 each year. Administrators for the registered entity (Entity Administrators) should receive a notice in early December to complete the Section 1600 Reporting Confirmation for the following year. If the Section 1600 Reporting Confirmation is not completed by the January 15deadline, the Entity Administrator will receive a second notice.

Once the annual Section 1600 Reporting Confirmation has been completed, entities will then begin to submit the required GADS, GADS Wind, TADS, and MIDAS data as appropriate. Timely data submission is extremely important in order for MRO staff to identify regional trends that could impact system reliability. This article is the first in a series that will delve into the reporting requirements of each Section 1600 data request individually and in depth. Stay tuned!

- Jake Bernhagen, PE, Senior Systems Protection Engineer

The Impact of FERC Order 881 on Facility Ratings

For this issue of Midwest Reliability Matters, MRO staff would like to share a newsletter article from our neighboring region, ReliabilityFirst. The article, written by Greg Sorenson, Senior Technical Auditor at ReliabilityFirst, discusses FERC Order 881 on Ambient Adjusted Ratings (AARs) which was issued by FERC on December 16, 2021. The article summarizes what will be required by various registered entities and some of the potential challenges that may require the development of new detective and preventative controls to assure the intent of the Order is being met accurately and reliably. The article is reprinted here with permission. Original source: https://rfirst.org/about/Newsroom/Newsroom Library/Issue 1 Jan-Mar 2022.pdf.

The purpose of this article is to highlight upcoming changes to facility ratings practices

On December 16, 2021, FERC issued Order 881. FERC Order 881 makes several changes to the expectations for facility ratings for transmission lines and power transformers under Section 206 of the Federal Power Act, which establishes the Commission's powers to fix rates and charges.[1] [NERC Reliability Standard] FAC-008-5 requires a

[1.] Section 215 of the Federal Power Act relates to Electric Reliability.

methodology for Transmission Owners. As the implementation period proceeds, Transmission Owners under FERC jurisdiction should modify their methodology as required by the Order and their Transmission Provider.

Transmission Owners are also encouraged to review and update their internal controls to ensure accurate ratings at all times. Facility Ratings are important inputs into real-time operations, peak hour planning, numerous operational and transmission planning studies, the market dispatch system, protection system settings, and the sale of transmission service. Overly conservative transmission ratings can lead operators to make well-intentioned but incorrect decisions due to the near-term transfer capability not accurately portraying the System, which can lead to restricted flows and increased congestion costs that are not valid. The physical capabilities of the transmission facility are affected by many factors that are different in real time from seasonal assumptions; Order 881 requires an Ambient Adjusted Rating be established for each clock hour on each transmission line, power transformer, and generator tie line. Entities may have to make modifications to their facility rating methodologies to reflect calculation of ambient ratings, separate day and night ratings, and unique normal and emergency ratings. Entities may have to make modifications to their processes to calculate[2] ratings based on environmental conditions changing (updating these ratings at least hourly).

FERC Order 881 requires the use of Ambient Adjusted Ratings, which improve performance of the Bulk Electric System by more accurately reflecting the ability of transmission lines to transfer power under current conditions rather than seasonal assumptions. An Ambient Adjusted Rating in FERC Order 881 considers the ambient air temperature and the solar irradiance when developing ratings. Specifically, the Transmission Provider must file an updated tariff that describes how Transmission Owners will develop the ambient-adjusted ratings.

"The physical capabilities of the transmission facility are affected by many factors that are different in real time from seasonal assumptions..."

At a minimum, FERC Order 881 requires that the Transmission Owners under FERC jurisdiction develop ratings that account for a large range of operation, from 10 degrees below the historical low to 10 degrees above the historical high. The rating must change at intervals no larger than 5 degrees; for those Transmission Owners already using them, this may significantly increase the number of Ambient Adjusted Ratings calculated. To reflect the lack of solar irradiance at night that leads to an approximately 10 percent increase in ratings, nighttime calculations need to exclude the effect of heating. Entities are expected to update the sunrise and sunset times at least monthly. Accurate temperature forecasts should be used to determine a temperature that the entity is sufficiently confident that the temperature will not exceed during the applicable interval. The calculated intervals cannot exceed one hour and the entity needs to calculate the next 240 hours; this calculation (or revalidation of the calculation) must be performed each hour.

Order 881 also requires that the Normal and Emergency Ratings be uniquely determined; different sets of assumptions will be used in order to develop ratings. Generally, equipment can withstand higher amounts of current for short periods of time. The system is typically operated to not exceed the Normal Rating under continuous conditions. The Emergency Rating is mostly used to ensure the system will not exceed this after a contingency occurs. The system should not exceed the Normal Ratings under normal conditions. As a result, nearly all Facilities are expected to have different Emergency Ratings than Normal Ratings. Transmission owners will have the

[2] Which can include consulting a look-up table, or validating that inputs remain the same once an hour.

discretion to determine the procedure to calculate emergency ratings but they must align with good utility practice and other requirements in the pro forma OATT Attachment M.

FERC Order 881 includes additional changes for seasonal ratings too. In particular, the seasonal ratings must have different day and night ratings, as well as uniquely derived normal and emergency ratings. Seasons are limited to three months in duration and at least four seasons are required. The Ambient Adjusted Ratings will be used for the sale of transmission service for periods ending within the next ten days. Additionally, the Ambient Adjusted Ratings will be used for transmission curtailment, interruption, and redispatch (including in market processes) within the next ten days. This will help ensure accurate information is used for operational decisions that affect a generator's ability to serve load. Seasonal ratings will be used for transmission service requests, including network service as well as transmission curtailment, interruption, and redispatch for requests that do not end within the next ten days.

Transmission Owners should review their existing internal controls around the facility rating process. Entities may also need to develop new detective and preventative controls to ensure accurate and consistent calculation of ratings at a variety of ambient air temperatures, day and night conditions, and in different seasons. In particular, new or improved controls may be needed to ensure calculations are performed correctly and on time, temperature data are correct, forecasting tools are functioning properly, and results are communicated to the appropriate parties and integrated properly into operational and transmission service tools. Entities are encouraged to periodically sample circuits within these tools to ensure ratings are properly represented.

While entities have three years to become fully compliant with certain components of Order 881[3], a number of factors need to be considered for a successful transition. Transmission Owners will need to work with their Transmission Providers to understand implementation details and timelines. The RF Entity Engagement and Assist Visit programs can help with questions entities have on how their implementation of the Order's requirements will impact their compliance programs for FAC-008 and other NERC Reliability Standards impacted by Facility Ratings (SOLs/IROLs, OPA, Real-Time Assessment, Facility Interconnection Studies, Transmission Relay Loadability, etc.

As a follow up to Order 881 on AARs, FERC issued a Notice of Inquiry (NOI) on February 17, 2022, which will query industry on the potential implementation of dynamic line ratings (DLRs). A DLR is a transmission line rating that applies to a time period of up to one hour and reflects forecasts or direct measurements of additional factors beyond ambient air temperature, such as wind, solar heating intensity, transmission line tension, or transmission line sag. MRO staff will provide a newsletter article summarizing the results of this NOI when they become available.

[3.] Please note that this article is not a comprehensive summary of potential compliance responsibilities introduced by FERC Order 881, nor does it constitute legal advice. This article summarizes important concepts, changes, and potential impacts from FERC Order 881. Entities should consult the Order for the specifics of its compliance impacts.

MRO 2021 Generator Winterization Program Results

In 2021, MRO staff surveyed Generator Owners in the MRO footprint to gain a better understanding of the generation profile in the region and the winterization practices underway for these facilities. Ten generating facilities responded to the survey, four of which were local to Saint Paul, Minnesota and hosted site visits by MRO staff. While the initial focus of the survey was on overall winterization preparations, additional emphasis was placed on each facility's generator winterization plan after the preliminary findings and recommendations from The February 2021 Cold Weather Outages in Texas and the South Central United States: FERC-NERC-Regional Entity Staff Report (February 2021 Report) were released.

A generator winterization plan should consist of seven key components: (1) safety; (2) management roles and expectations; (3) processes and procedures; (4) evaluation of potential problem areas with critical components; (5) testing; (6) training and (7) communications. These components are described in detail by NERC's Reliability Guideline: Generating Unit Winter Readiness – Current Industry Practices – Version 3. While not all of the facilities had a formal generator winterization plan, those facilities that didn't were performing a portion of the required activities. In addition, all of the entities whose plans were not complete, indicated they were working to formalize their winterization plans or are in the process of updating their plans in response to the latest recommendations from the February 2021 Report.

During the site visits and the interview process, MRO observed and learned about the efforts taken by the facilities in order to help assure their unit(s) would remain operational through the coldest weather they may experience. Some of the following steps taken were very basic, while others required significant capital investment:

- An additional insulating blanket covering already insulated and heat traced critical components on the northwest corner of the facility.
- The installation of air diffusers on the floor to redirect cold air drafts away from critical components.
- Use of insulating blankets and heaters on the steam turbine casing to decrease the turbine warm up time.
- The use of a radiant heating system to keep the combustion turbine air inlets clear.
- The installation of air manifolds in the combustion turbine air inlet filters to assist in lancing the filters.
- Building shelters for critical instrumentation, critical components such as boiler feed pump valves and for performing maintenance activities on top of the boiler.
- Enclosing and heating the entire facility.

Heat tracing and insulation are two key measures to prevent the freezing of critical components and were widely used by all of the facilities surveyed. One key difference noted between facilities was how heat tracing was monitored. Heat tracing can be monitored by voltage (lights at the end of the circuit indicating the circuit is energized), or by current. Current monitoring varied by site, with some sites taking readings to prepare for the season and on a set periodicity throughout the winter, while other facilities have continuous current monitoring. MRO discovered, while indicator lights at the end of each circuit are a great way of to verify the circuit is

energized, current monitoring is an indicator of when a circuit is starting to fail as the current flow starts to decrease. In addition, there seems to be a trend for facilities to start monitoring heat trace systems from the generator management systems as upgrades are being made. The focus of MRO's Generator Winterization Program in 2022 will include:

- Reviewing Generator Winterization Plans.
- Evaluating whether recommendations from The February 2021 Report are being implemented.
- Assessing the implementation status of NERC Alert recommendations.

One of MRO's goals for 2022 is to complete six generator site-visits, targeting at least three in the southern region of the MRO footprint and request ten additional generators to participate in the Generator Winterization Program survey. For questions on this important program, please submit emails to GWP@mro.net.

- Russ Mountjoy, Principal Reliability Specialist

Industry Tips and Lessons Learned

Seven new lessons learned have been posted on the Lessons Learned page of NERC's website on the following topics:

- Intermittent Network Connection Causes EMS Disruption
- Unintended Consequences of Altering Protection System Wiring to Accommodate Failing Equipment
- Substation Flooding Events Highlight Potential Design Deficiencies
- Model Data Error Impacts State Estimator and Real-Time Contingency Analysis Results
- Islanding and Insufficient Primary Frequency Response Resulted in Unintended UFLS
- Distributed Energy Resource Performance Characteristics during a Disturbance
- Managing UFLS Obligations and Service to Critical Loads during an Energy Emergency

NERC also publishes compliance guidance to provide a common understanding among industry and ERO Enterprise Compliance Monitoring and Enforcement Program staff of how compliance can be achieved and demonstrated. These guidance documents can be found on the Compliance Guidance page of NERC's website.

MRO TO HOST 2022 RELIABILITY CONFERENCE

May 18, 2022 | 8:00 a.m. to 4:00 p.m. Central | In-Person or Virtual

Conference Details

MRO's Reliability Advisory Council invites you to attend the 2022 Reliability Conference, which will be held at the InterContinental Kansas City at the Plaza in Kansas City, MO. This much anticipated one-day conference will focus on bulk power system 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.

Agenda Topics

The agenda is now available on our website and includes the following topics:

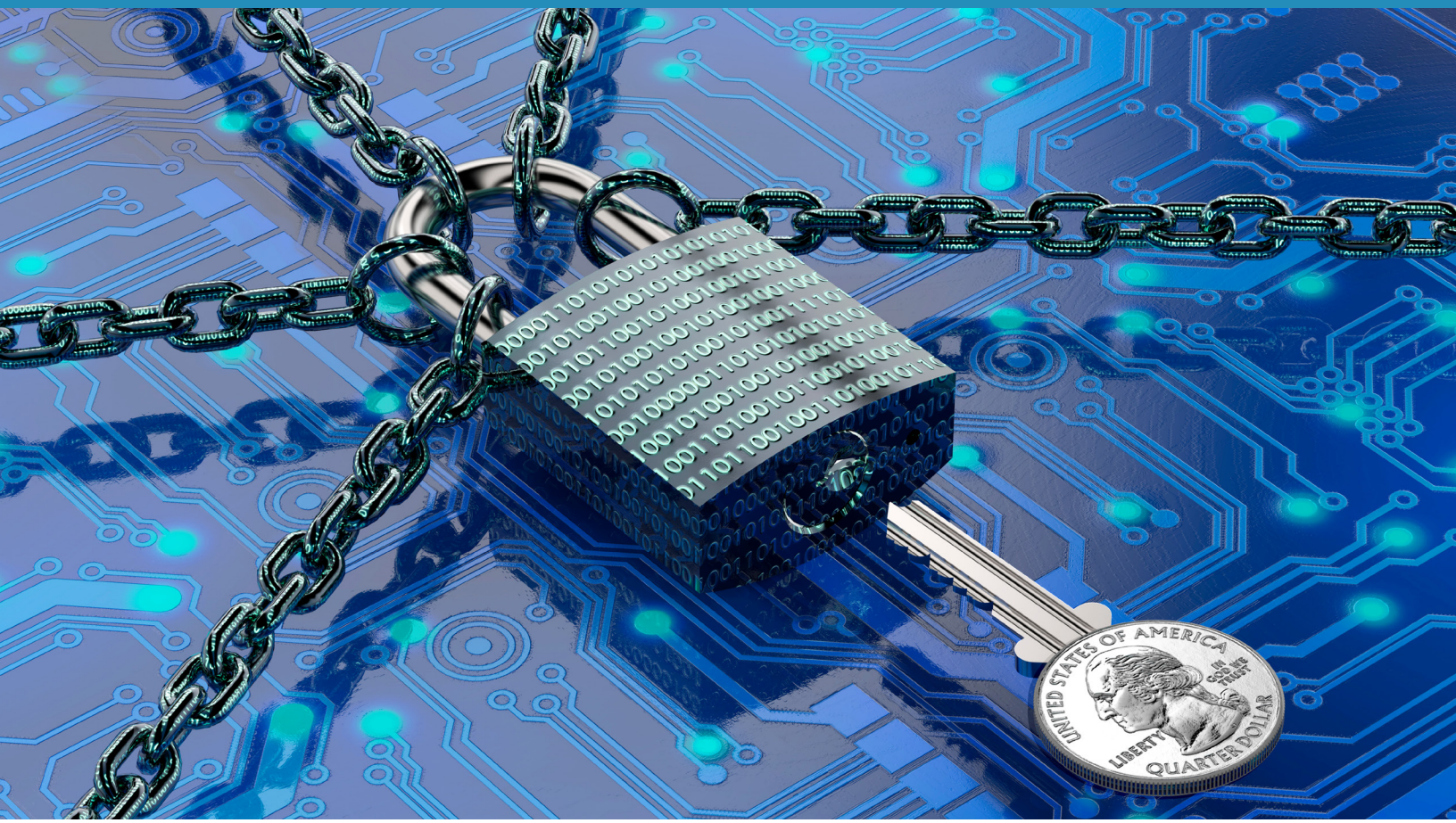
- Energy Assurance and Assessment Methods Across the ERO Enterprise
- MISO/SPP Joint Transmission Planning Projects
- Ambient Adjusted Ratings Implementation
- OGE System Zonal Study for Voltage/VAR Control
- Grain Belt Express Transmission Project

Registration and Lodging

Registration is now open and closes on **May 11, 2022**. Rooms can be reserved at the InterContinental Kansas City at the Plaza at a rate of $164/night. (Room rate will be applied when booking.) Hotel room block expires on April 27, 2022.

There will be a social networking event at the InterContinental Kansas City at the Plaza on May 17, 2022 from 5:00 to 7:00 p.m. Central (appetizers will be provided and a cash bar available).

SECURITY CORNER



Cyber Attack for Ransom

How this threat has evolved and what to do today

Cyber attack for ransom (CAFR), also broadly known as “ransomware” has been evolving from its most basic form since 1989. There was a large uptick in ransomware activity in 2013, with the primary vector being a malware-based drive-by or a social engineering attack that would trick users into downloading and installing ransomware that encrypted the user’s files. In 2020, the sophistication of CAFR increased exponentially and includes the concurrent methods described below.

Evolution of Methods

It is important to recognize the evolution of methods and the increase in sophistication of today’s CAFR activities. Cybercriminal and nation-state actors have progressed from drive-by downloads to encrypting data automatically through the deployment of ransomware as one of many adversarial actions a criminal will take to accomplish the overall objective. The latter scenario requires a much deeper incursion into the infrastructure of a business. This approach by the adversary significantly increases the effectiveness of the ransom demands because countermeasures to standard controls and mitigations that usually prevent unauthorized encryption of data can be deployed. Examples of the standard controls include things such as online and nearline (on-site storage of data on removable media) backups of data, or administrative access to sensitive business and operational systems. This has the practical effect of heightening the overall impact of the

ransomware deployment. It is important to understand how the pursuit of increased attack sophistication has been driven by a motivation of direct and immediate financial gain - profit. In the early days of CAFR, the adversary deployed a malicious software that automatically encrypted exposed data, sometimes with a static encryption key. If the victim was unprepared for such an event and did not maintain viable standard forms of IT backups, the adversary's potential for monetization was intact. However, for victims that maintained the most basic principles of data backup and redundancy, a simple restore of the affected dataset rendered the monetary possibilities for the attacker ineffective. To increase the chance of operational success and ultimately a monetary reward, the attackers had to find more avenues for monetization and ensure common controls available to victims are neutralized before performing actions on objectives. This is considered the genesis for the evolution from *ransomware* to CAFR.

Modes of CAFR

Some of the monetization avenues these modes of attack seek are obvious, some are not. As such, they deserve discussion and understanding. The following table summarizes recognized, evolved methods that are used for deployment of CAFR.

Mode	Impacts
Denial of Service (DOS) for Ransom	Temporary resource exhaustion, adverse operational impacts
Denial of Data for Ransom	Inability to perform critical business functions, like Accounts Payable/Receivable
Reputation for Ransom	Publication of embarrassing or sensitive information
Operations for Ransom	Inability to ensure continuity of operations

CAFR is inherently designed to extract monetary value from firms, usually in the form of hard-to-track cryptocurrency. To increase success rates, criminals have evolved tactics, techniques, and procedures (TTP's) and integrated individual lessons learned into their operational capabilities. As the attackers' operational capabilities have matured, they have moved operations beyond targets of opportunity to targets in the Critical Infrastructure (CI) sectors in the U.S. Firms in any one of the 16 sectors recognized as CI are particularly enticing targets because of the perpetual nature of their operational requirements, the broad economic reliance on the firms in these sectors, the massive population base that requires the services of these firms on a minute-by-minute basis, as well as the U.S. Government's reliance upon partnerships with private firms in these sectors to support all missions world-wide. At the time of this writing, CAFR has been observed in all 16 Critical Infrastructure sectors in the previous 12 months. The attackers have concluded that the more pressure there is for an organization to *operate in perpetuity*, the better the adversary's chances are of being rewarded for their efforts - they can use a company's core services operational requirements as leverage to encourage ransom payments.

The TTPs employed by the adversary support what many would consider a *full breach* approach in their attacks within the Critical Infrastructure space. The attackers are infiltrating organizations, living-off-the-land, and ensuring adversarial advantages by assessing the posture of the organization, defeating controls, and preparing the victim infrastructure to maximize monetary possibilities. This approach implies, and requires, a true understanding of the target organization's systems, which in turn implies a longer-term presence for the purposes of reconnaissance. The following sections provide additional detail of specific approaches denoted in the above table used for monetization.

Monetization: Reputation for Ransom

Attackers are exfiltrating copies of data and analyzing it for sensitive information, which can be called upon for a publish-for-ransom scheme either as proof to the victim organization that they have been compromised, or as an alternative for ransom if the victim has common controls and backups in-place to ensure continuity of operations. This is referred to as *Reputation for Ransom*.

Monetization: Data for Ransom

Manipulation of online and nearline IT backups by the attackers ensures the victim has no practical common response capabilities and helps the attacker apply maximum pressure for a ransom payment, then allowing the victim access to encrypted data required for day-to-day operations.

Monetization: Operations for Ransom

Within the Critical Infrastructure sectors in the U.S., the primary missions served require 24X7x365 operational continuity. The attackers exploit this requirement by attempting to control, corrupt, or otherwise disrupt Industrial Control Systems (ICS) that are used to control processes or infrastructure related to the ability of the firm to deliver their product to the broad population. This is the most alarming and perhaps the most effective use of CAFR by the adversary. The most recent examples of this mode of attack have been very successful in extracting monetary value from firms like Colonial Pipeline and JBS Meatpacking. Therefore, there is little reason to believe this mode will not continue to be extremely effective for attackers.

Monetization: Victim Access to Foreign Intelligence Services and Nation States

A non-obvious avenue of monetization is cybercriminals providing access to full breach victims to foreign intelligence services and nation states. There have been instances of multiple teams attacking the same victim, but with different objectives. This is indicative of cybercriminals operating alongside foreign intelligence services, but to different ends. This leads to a potentially symbiotic relationship amongst cybercriminals and the foreign intelligence services which are co-opted through a monetary relationship and encourages tacit approval for cybercriminal operations by governments and nation states.

A Sense of Urgency

CAFR has changed the landscape beneath our feet, recently and rapidly. A proactive, planned, practiced response is the most effective approach available to the incident response team. A precise focus on the operational requirements of not only a company's systems, but also the functional components of those systems and the tactical response objectives required to ensure continued operation of those components is needed. This approach ensures that response activities are not only focused on the essential perceptions of ransomware and CAFR, but introduce a capability to adapt to the ever increasing sophistication of these threats. It is now essential to consider operational requirements anchoring the response strategy. With this deeper understanding of system interaction, one can ensure the possibility of operational success even in the face of escalation of a sophisticated threat.

Summary

The CAFR strategy focuses on ensuring restoration capabilities for data systems and isolation of critical functions into zones of sustained operations. These zones must be able to operate independently of one another to ensure operational continuity of unaffected critical functions during response activities. Departure

and return of normal operational conditions must be well planned and continually practiced. The foundational capabilities of data restoration and protective isolation are the keys to our success when responding to a CAFR.

- Michael Meason, Sr. Manager, Information and Security, Western Farmers Electric Cooperative and MRO SAC Vice Chair

About the Author

Michael Meason, Sr. Manager, Information and Security, Western Farmers Electric Cooperative

Michael Meason, Senior Manager, Information and Security, for Western Farmers Electric Cooperative was promoted to his current role in June 2018.

He began his career at Wester Farmers Electric Cooperative 11 years ago as a Senior Network Engineer and has also served as the Manager of Technical Services.

Michael has 10 years of experience in enterprise information technology (IT) and cyber security within the Financial Services Sector, in addition to 11 years of experience in the Electric Utility Industry.

His areas of influence include information technology (IT), operational technology (OT), telecommunications engineering, and network.

About the Security Advisory Council

MRO's Security Advisory Council (SAC) is made up of industry volunteers from MRO member companies. These subject matter experts provide advice and counsel to MRO's Board of Directors, staff, members, and registered entities regarding: (1) cybersecurity; (2) physical security; and (3) SCADA, EMS, substation and generation control systems.

The SAC provides outreach and promotes awareness in these three key security areas. More information on the SAC can be found on MRO's website.

OPERATIONAL UPDATE

Navigating Spring Mud

For many individuals, especially those of us that live in colder climates, spring is a favorite season. We look forward to the disappearance of snow, the resurgence of vegetation, and the onset of warmer weather. While I am an avid golfer and definitely appreciate the end of snow shoveling season, I have never been one that fully embraces spring. I suspect this is largely due to my time growing up on a farm, and this time of year signaling to me (or more so my Dad) that it was time for me to transition my focus from basketball, ice fishing, and school to farm work. Or, maybe it's the type of farm work that takes place in the spring I dreaded so much – cleaning grain bins, getting equipment ready for planting, and above all – dealing with lots and lots of mud. Sometimes that meant putting my early engineering mind to work on how to get unstuck without the benefit of a tow vehicle in the middle of nowhere (before cell phones), and other times it meant being realistic about getting the work done versus doing more harm than good by rutting up a field.

This spring feels different to me. I just finished spending a few days with MRO colleagues and a number of our board members in person for a hybrid board meeting. This was the first time MRO has hosted non-staff at our offices in well over two years. The meeting went fantastic, largely due to the thoughtful planning and testing that a number of MRO staff undertook to ensure that this was truly a hybrid meeting as opposed to

an in-person meeting with remote capability. While it was great to take part in this new meeting format, the opportunity to socialize with those who attended in person and discuss things that weren't on the meeting agenda meant a lot to me. I look forward to reconnecting face-to-face with all of our board members in the months ahead.

I will have a similar opportunity in the coming weeks to reconnect with peers across the ERO Enterprise as we gather together in-person for the first time since early in 2020. I'm looking forward to seeing these colleagues face-to-face, and to socializing and sharing ideas that further the important mission of the ERO Enterprise. In May, MRO is hosting its annual Reliability Conference in Kansas City. This will be MRO's first in-person outreach event since October of 2019 and will be followed by the first in-person meeting of the Reliability Advisory Council (the organizational group responsible for putting on the conference) in the same timeframe. These events are being offered in a hybrid format, and like the last board meeting, a lot of thought and planning is going into making sure both in-person and virtual attendees have a comparable opportunity to participate. MRO also plans to resume on-site Compliance Monitoring and Enforcement Program (CMEP) activities in May, and the NERC Board of Trustees recently announced that its second quarter meeting will be in-person, with guests.

All of these events signal a welcome shift in how we have been operating since the onset of the pandemic. This is likely why this particular spring feels so different to me. The lifting of health restrictions and a return to some of my favorite in-person activities has been a breath of fresh air. Consistent with the spring season, a rebirth of sorts is underway in how we consider engaging with each other in the future. Leaning into what we've learned over the past 24 months about connecting virtually, along with the benefits we know exist from in-person interaction, will help us implement a "best of both worlds" approach that continues to support our shared vision of a highly reliable and secure North American bulk power system.

The past two years might best be described as the "muddy season," where we all had to be extremely thoughtful and creative in our approach to just getting the work done. The spring of 2022, however, is finally presenting us with unique opportunities to reconnect and re-envision the best path forward out of the mud.

Thank you for your support in helping us ensure the reliability and security of the grid!

-Richard Burt, Senior Vice President and Chief Operating Officer

INDUSTRY NEWS AND EVENTS

LATEST NEWS:

DOE Seeks Applications, Bids for $6 Billion Civil Nuclear Credit Program

On April 19, 2022, the U.S. Department of Energy (DOE) announced plans to seek applications and sealed bid submissions under the $6 billion Civil Nuclear Credit Program (CNC) to support the continued operation of U.S. nuclear reactors — the nation's largest source of clean energy. See the full announcement.

FERC Presentation | Building for the Future Through Electric Regional Transmission Planning and Cost Allocation and Generator Interconnection

The Federal Energy Regulatory Commission (FERC) issued a draft NOPR related to regional transmission planning and cost allocation requirements that would work to remedy deficiencies in the Commission's existing process and requirements. See the full announcement.

FERC Seeks Information on Organized Markets' Changing System Needs, Plans

On April 21, 2022, FERC took the next step toward modernizing wholesale electricity market design by directing the operators of six regional organized electric power markets to provide information regarding their changing system needs and plans for potential reforms. See the full announcement.

Industry Experts Author Paper on Climate Change Impacts to the Grid

Mark Lauby, NERC senior vice president and chief engineer, co-authored and reviewed a report on the grid and climate change as part of IEEE's, Power & Energy Society (PES) Industry Technical Support Leadership Committee (ITSLC). See the full announcement.

Operational Communication, Collaboration and Coordination Key to Industry Success during an Event

Enhancing routine and emergency operations coordination between the electricity industry and natural gas providers is one of several recommendations identified during NERC and the Electricity Information Sharing and Analysis Center's (E-ISAC) sixth security exercise, GridEx VI, held in November 2021. See the full announcement.

NERC Report Highlights Criticality of Ensuring Reliable Operation of Inverter-Based Resources; Provides Recommendations

The ongoing widespread reduction of solar photovoltaic (PV) resources continues to be a notable reliability risk to the bulk power system (BPS), particularly when combined with the loss of other generating resources on the BPS and in aggregate on the distribution system, a joint report from NERC and WECC found. Read the full announcement.

INDUSTRY EVENTS:

Talk with Texas RE: FAC-008

May 5, 2022 | 1:30 to 2:30 Central | Virtual

This presentation will cover FAC-008 and common themes in facility ratings methodology, evidence, and issues. Register here.

Industry Webinar: Multiple Solar PV Disturbances in CAISO (Disturbances between June and August 2021: Joint NERC and WECC Staff Report)

May 10, 2022 | 1:00 to 3:00 p.m. Eastern

NERC and WECC recently published a joint report—Multiple Solar PV Disturbances in CAISO Disturbances between June and August 2021: Joint NERC and WECC Staff Report—regarding four disturbances involving the widespread reduction of

power from bulk power system (BPS)-connected solar photovoltaic (PV) resources that occurred in Southern California, specifically in areas of high penetrations of solar PV and wind resources. This webinar is intended to answer questions about the report's findings. Register here.

Talk with Texas RE: FERC and ERO Enterprise Joint Review of Protection System Commissioning Programs Report

May 10, 2022 | 1:30 to 2:30 Central | Virtual

Guest speakers from FERC and NERC will discuss the November 2021 FERC, NERC, and Regional Entity Staff Joint Review of Protection System Commissioning Programs. Register here.

NERC Board of Trustees, Board Committees and Member Representatives Committee Meetings

May11-12, 2022 | Arlington, VA

Register here.

NPCC 2022 Spring Compliance and Reliability Webinar

May 17, 2022 | 9:00 to Noon Eastern | Virtual

Register here.

SERC Natural Gas and Electric Coordination Vision for the Future Webinar

May 17, 2022 | 9:00 to Noon Eastern | Virtual

The webinar will provide a forum for experts in the gas industry, as well as electric utilities planning groups to raise awareness as we work together to understand and address the risk to reliability. Register here.

SERC Ransomware Webinar

June 15, 2022 | Virtual

The focus of this event is to create awareness on Ransomware as a major risk to all critical infrastructure as well as the electric utility industry. Register here.

MRO EVENTS:

Annual Reliability Conference

May 18, 2022 | 8 a.m. - 4 p.m. Central

MRO's Reliability Advisory Council is hosting this event at the InterContinental Kansas City at the Plaza in Kansas City, Missouri. Attendance is also available by web. Read more and register here.

Reliability Advisory Council Meeting

May 19, 2022 | 8:00 a.m. Central

Held in person in Kansas City, Missouri. Register here.

CMEP Advisory Council Meeting

June 7, 2022 | 8:00 a.m. to 3:00 p.m.Central

Format TBD. Register here.

Security Advisory Council Meeting

June 22, 2022 | 8:00 a.m. to 3:00 p.m.Central

In-person at MRO's offices in Saint Paul, MN. Register here.

Board of Directors and Board OGOC Meetings

June 22-23, 2021 | Saint Paul, MN

The board's Organizational Group Oversight Committee meets in person on June 22 at MRO's Saint Paul offices. Virtual attendance is also an option. Register here.

The board of directors meets on June 23 in person at MRO's Saint Paul offices. Virtual attendance is also an option. 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