APRIL 2021

"Spring is proof that there is beauty in new beginnings."

-Matshona Dhliwayo

# MIDWEST RELIABILITY MATTERS

# Inside This Issue



**DISCLAIMER**

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

# CEO MESSAGE

# Ushering in Spring

## The season of change and revitalization

I recently read a poem by Laura Kelly Fanucci that resonates with me. It articulates the resilience we have collectively experienced over the past year and hope for what the future will bring.

*May we never again take for granted*
*A handshake with a stranger*
*Full shelves at the store*
*Conversations with neighbors*
*A crowded theater*
*Friday night out*
*The taste of communion*
*A routine checkup*
*A school rush each morning*
*Coffee with a friend*
*The stadium roaring*
*Each deep breath*
*A boring Tuesday*
*Life itself.*

*When this ends,*
*May we find*
*That we have become*
*More like the people*
*We wanted to be*
*We were called to be*
*We hoped to be*
*And may we stay*
*That way—better*
*For each other*
*Because of the worst*

*-Laura Kelly Fanucci*

It's hard to believe that more than a year ago we first responded to the global COVID-19 pandemic—prioritizing the health and safety of MRO staff and the continuity of operations—while at the same time providing regulatory relief to allow industry to do the same. Shortly after, we responded to civil unrest that tested the core values of who we are as a nation…and as a community. George Floyd's death in Minneapolis made it abundantly clear that diversity, equity and inclusion aren't just words on paper, they are verbs that require our action. Work continues at MRO to not only raise awareness amongst staff, but to also address the inequities that inherently exist in our systems. Then in December, we responded to a significant supply chain compromise and the potential security risk posed to our industry. The Electricity Information Sharing and Analysis Center, along with NERC and the Regional Entities, acted quickly and in coordination with industry and government partners to assess the situation and safeguard the security of the North American bulk power system.

I had hoped that because 2020 came in like a lion, it would leave like a lamb. That certainly has not been the case. The cold weather that encompassed our region in mid-February led to unprecedented reliability challenges with wide-ranging impact across the "middle south" states and Texas. During the event, system loads were high, generation was unavailable, and fuel supply was limited. Energy emergencies were declared across the MRO region, and load shedding occurred in the ERCOT, MISO, and SPP operating areas. NERC and FERC announced a Joint Inquiry into the event that MRO will participate in. On its heels, we learned of another significant cyber concern related to Microsoft Exchange.

The challenges we faced over the past twelve months have indeed, been significant.

These challenges highlight this industry's resilience. One of the keys to our success is an ability to quickly respond to address rapidly evolving risks to the reliability and security of the North American bulk power system. The past twelve months have unfortunately provided us plenty of practice in this regard.

For the ERO Enterprise, our resiliency has been further strengthened by the transformational journey we embarked upon in 2019 to improve our connectedness and collaboration. This effort has transformed the way we work together to execute our mission. Considerable effort across the enterprise has been dedicated to the success of this initiative and NERC and the Regional Entities are more aligned now than ever before. The commitments we made to each other and to our collective success prepared us well to respond to the difficult circumstances we faced this past year.

As we move into the spring season, it's hard not to be optimistic about the future. The sun is warmer, the days are longer, the fields are greener…transformation abounds! Spring is the season of change and revitalization. It brings hope of brighter days ahead. In early May, MRO will begin reopening the newly refreshed and remodeled Saint Paul office. Our staff will again have opportunities to connect with colleagues, peers, and friends without peering through a computer monitor.

Spring is yet another reminder that change is inevitable. As we enter this next chapter, let us build upon the experiences and lessons learned from the past year. Let us build upon the connections and continue to cultivate the relationships that are so important to our collective success. As Laura Kelly Fanucci said in her poem, "[m]ay we be better for each other because of the worst."

***Our future is bright!***

*- Sara Patrick, President and CEO*

# Employee Spotlight

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

Julie Peterson joined MRO in January as Assistant Corporate Secretary and Senior Counsel. Julie has several years of experience serving as corporate secretary for a global payment technology associaton and brings significant corporate governance and legal knowledge and skill to the organization. Julie received her undergraduate degree from the University of North Dakota and her J.D. with distinction from the University of North Dakota School of Law.

Joel Liu joined MRO in January as an Operations Compliance Engineer III. Joel's extensive background in transmission planning, studies and modeling are a valuable asset to MRO's compliance team, and we are already benefitting from his expertise!

Kendra Buesgens also joined MRO in January as Risk Assessment & Mitigation Administrator for the RAM team. Kendra brings six years of experience in a variety of roles that include recruiting, training, and support.

Hyder Memon joined MRO in March as an Operations Principal Compliance Engineer. Hyder has 17 years of experience in engineering and project management and holds a P.E. in Alberta and Minnesota. We are excited to welcome Hyder to our compliance team!

**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 (COPs)*

A COP is an oversight strategy for a registered entity that provides comparative assessments to shape oversight planning and resource allocation for Electric Reliability Organization (ERO) Enterprise staff, and places emphasis on understanding internal controls and other performance considerations of a registered entity. MRO's process for developing COPs requires input from the Reliability Analysis (which includes Registration), Risk Assessment and Mitigation, Compliance, and Enforcement Departments. The resulting COP from this process documents MRO's holistic assessment of the registered entity's inherent risk and the performance considerations assessing the entity's management of its risk. The COP guides MRO's monitoring activities for that individual entity. MRO currently has completed 62 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 implemented a schedule to complete the remaining 38 percent by year's end. MRO continues to innovate the COP process and is working on a streamlined COP approach for low-inherent risk entities. MRO is also developing tools for analyzing COPs across multiple organizations to identify trends and develop outreach opportunities, which will be utilized annually.

*2021 Compliance Audit Status*

MRO completes periodic Compliance Audits to assess registered entities' compliance with the NERC Reliability Standards. MRO staff has completed five scheduled Compliance Audits for 2021. MRO will provide resources and participate in coordinated oversight audits led by other Regional Entities, but has not participated in any in 2021 thus far. Coordinated oversight is a joint engagement with other Regions for ERO approved multi-regional registered entities. Coordinated oversight 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. Please visit MRO's website to view MRO's 2021 audit schedule.

MRO continues to perform all audits remotely and plans to do so through at least Q2 of 2021. 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.

*2021 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 the MRO Regional Risk Assessment and the ERO Enterprise CMEP Implementation Plan are 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 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 375 questions since it started in November of 2016. Over the last quarter, MRO has received 25 HEROs questions with an average response time of 10 days. This average is significantly better than the 30-day response goal.

*Expanded COVID-19 Reporting Guidance*

The ERO Enterprise has expanded regulatory discretion to include any potential noncompliance between March 1, 2020, and June 30, 2021, where COVID-19 contributes materially or completely to the root cause. The ERO Enterprise recognizes the fluidity of this emergency and will reassess the timeline if needed.

In the event that a potential noncompliance was caused by COVID-19, MRO registered entities should report the issue through MRO's enhanced file transfer server using the NERC-provided COVID-19 reporting template. Because COVID-19-related noncompliance is eligible for regulatory discretion, the established processes for self-logging /self-reporting noncompliance are not necessary for these issues. This additional level of monitoring, provided by MRO, assists registered entities in prioritizing compliance activities during the pandemic. For more guidance on this process, please refer to the information provided in MRO's Hot Topic.

*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, 2021, there are 31 MRO entities participating in the Self-Logging program, which accounts for 34 percent of all ERO Self-Logging participants, more than any other Region. Self-Logged instances submitted by these participants are monitored separately as the program is designed to quickly resolve minimal risk issues that were self-identified by entities. These issues are presumed minimal risk Compliance Exceptions (CE), however, the final disposition is based on a RAM risk determination. MRO is continually evaluating its process and outreach to improve processing efficiencies and validation of minimal risk noncompliance.

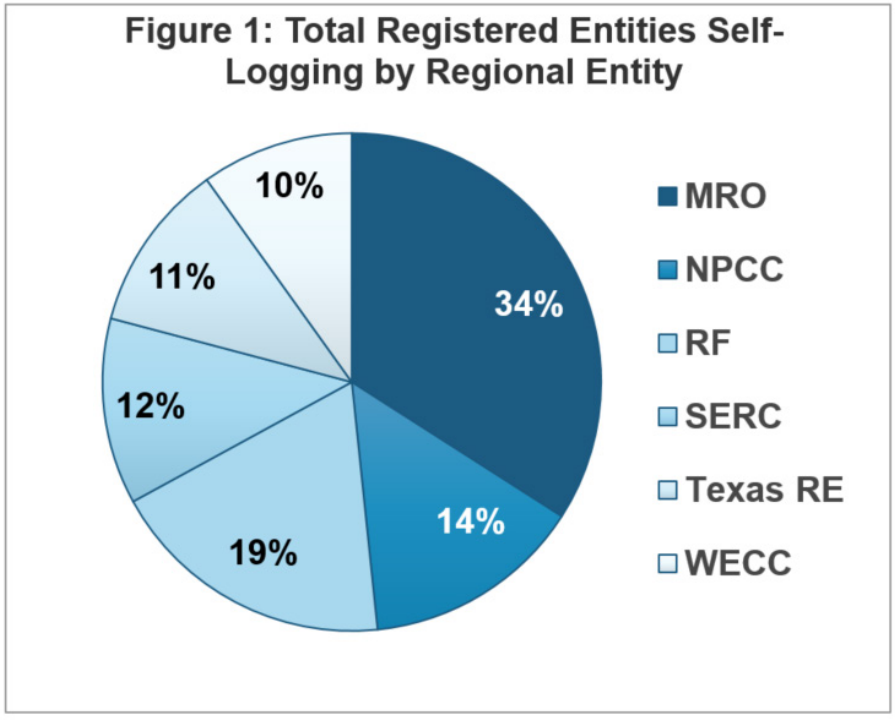
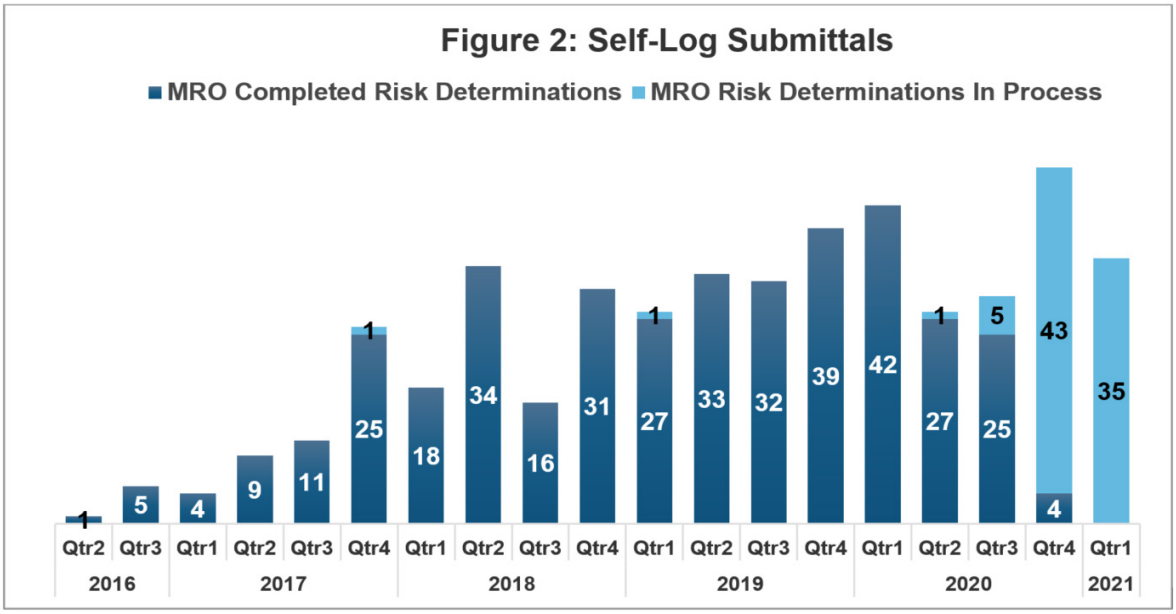


Figure 2: Self-Log Submittals illustrates self-logged instances of noncompliance by submittal dates. The two self-logs prior to 2020 have complicated mitigating activities and are approaching completion. Please note submittal dates are not the start of potential noncompliance or when MRO completed its risk determination analysis.

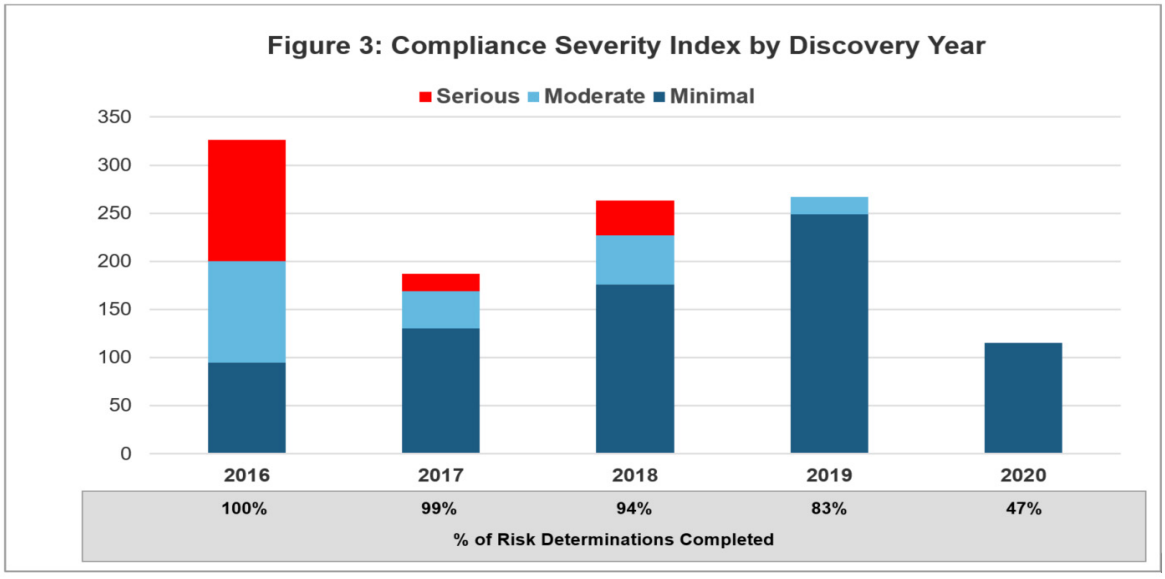



## Risk Assessment and Mitigation Trends

In the following Risk Assessment and Mitigation Trend charts and statistics, the numbers reflect all historic noncompliances in the expanded MRO region.

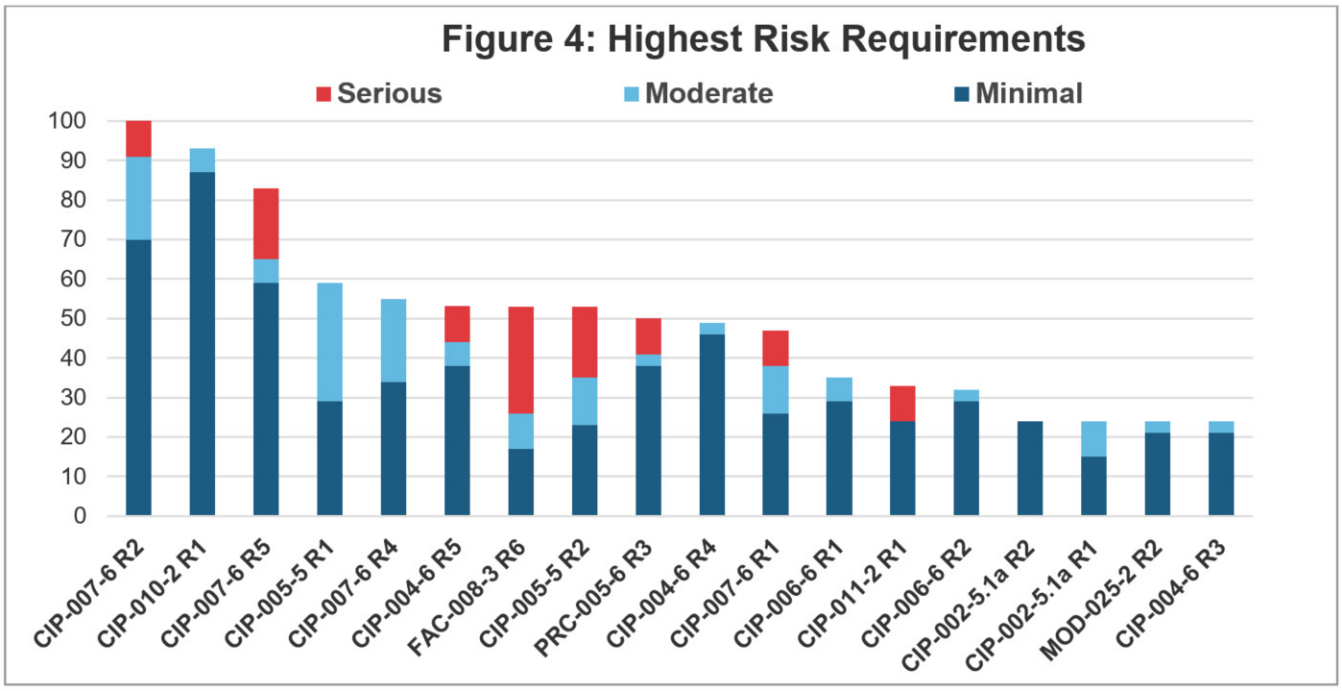
*Compliance Severity Index (Figure 3)*

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 noncompliance instances 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. For more information on how this process was developed and implemented, please see the article on "The Benefits of Risk-Based Regulation." MRO has seen a notable decrease in the risk of noncompliances 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.



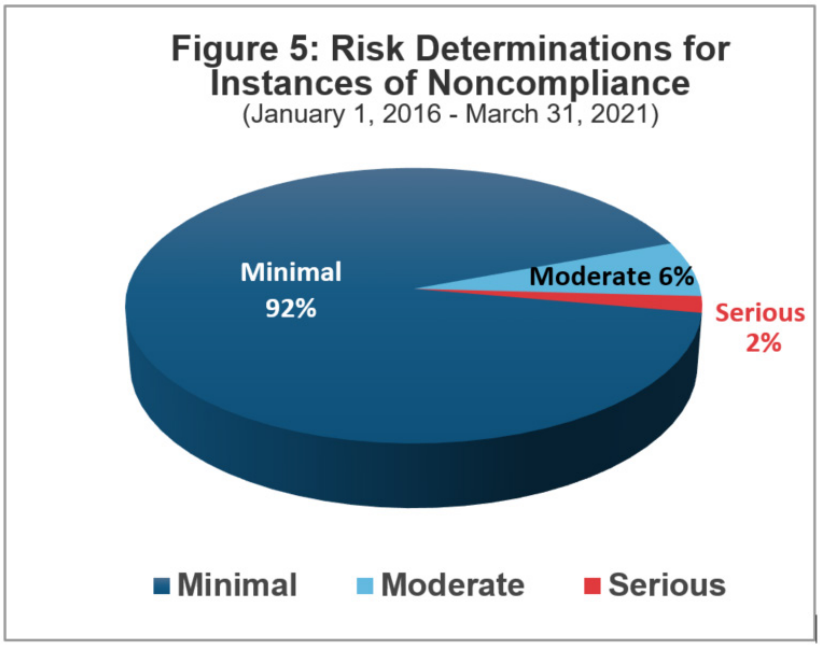
*Highest Risk Noncompliances (Figure 4)*

Figure 4 provides the 15 highest risk requirements, from January 1, 2016, to March 31, 2021, that have a history 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.




*Risk Determinations of all Instances of Noncompliance (Figure 5)*

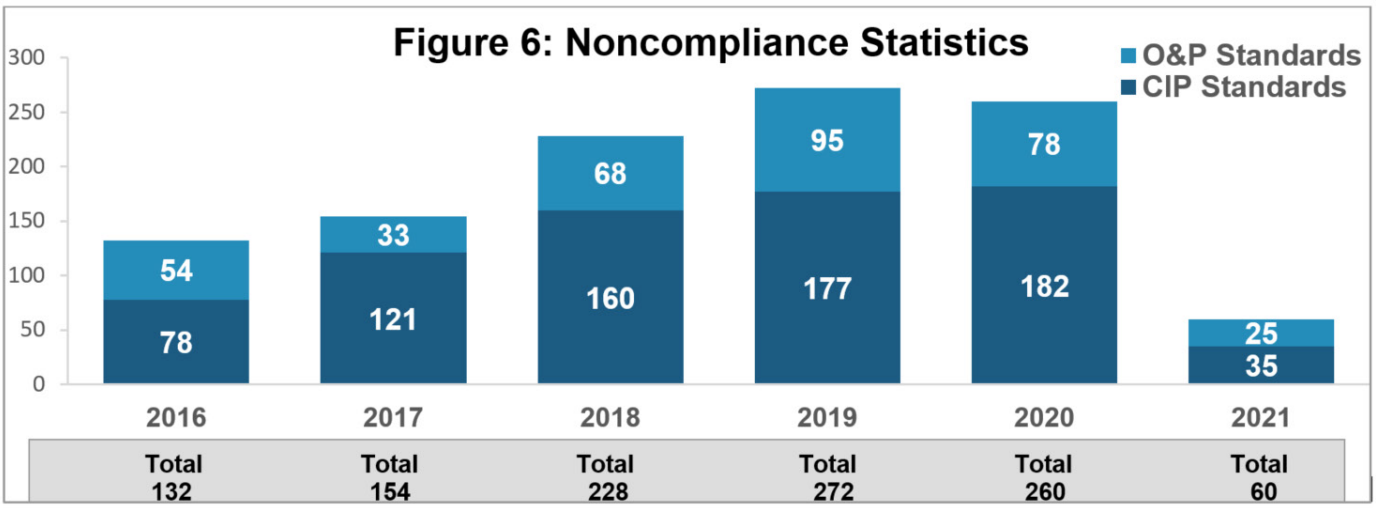
Ninety-two percent of all instances of noncompliance from January 1, 2016, to March 31, 2021, were minimal risk. There is a correlation between the increasing percentage of noncompliances being minimal risk (Fig. 5) and the increasing percentage of self-reported noncompliance (Fig. 7). Entities are identifying noncompliance earlier before the issues become more impactful to the reliability and security of the Bulk Electric 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 are annually discovered and reported to NERC from January 1, 2016, to March 31, 2021.




*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 noncompliances in order to prevent future noncompliance with NERC Reliability Standards.

Figure 7 reflects instances of noncompliance that MRO processed from January 1, 2016, to March 31, 2021.

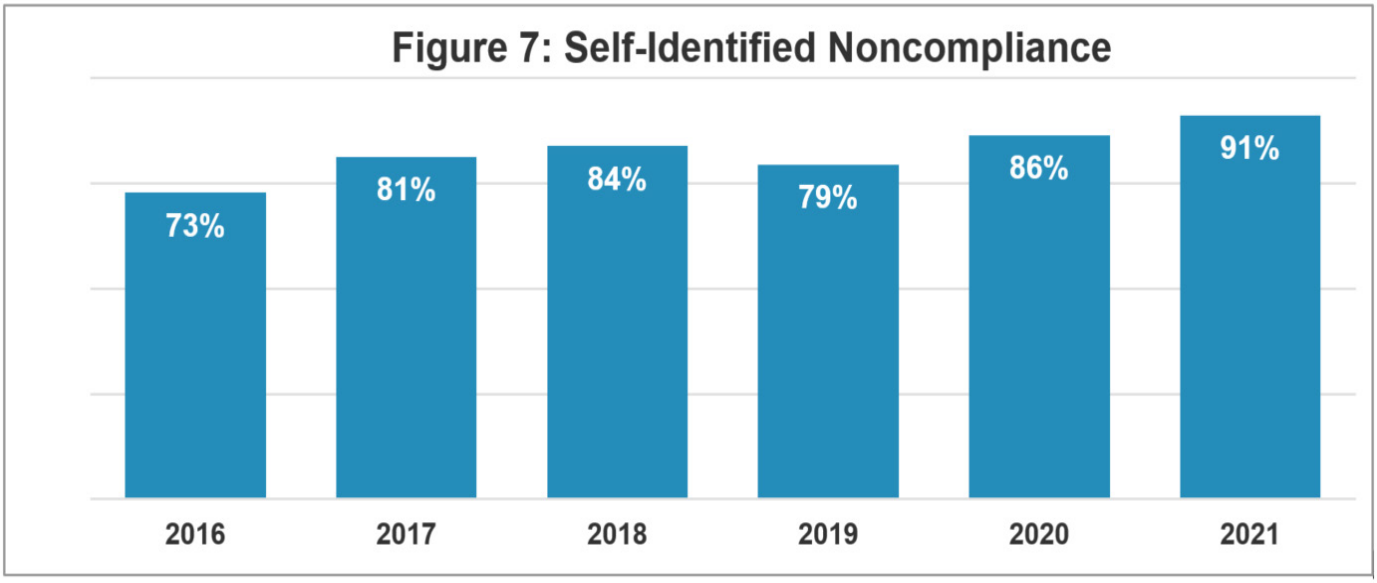
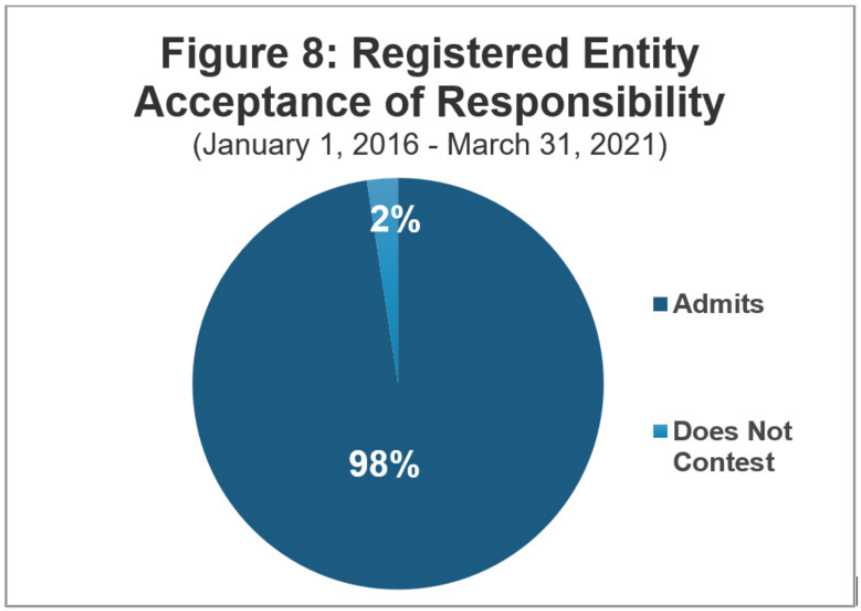


Figure 8 shows the percentage of time that registered entities have accepted responsibility for noncompliance submitted to NERC or another applicable Regulatory Authority from January 1, 2016 through March 31, 2021.




*Discovery Method Detail (January 1, 2016 through March 31, 2021) (Figure 9)*

In Figure 9, the numbers reflect all noncompliances in the MRO region that were reported to NERC.

**Figure 9: Discovery Method**

| Discovery Method Detail | 2016 | 2017 | 2018 | 2019 | 2020 | 2021 | Sub Total | (-less) Dismissed | Total |
|---|---|---|---|---|---|---|---|---|---|
| **Compliance Audit** | 25 | 26 | 33 | 47 | 39 | 0 | 170 | 18 | 152 |
| **Compliance Investigation** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **Data Submittal** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **Self- Certification** | 11 | 2 | 23 | 9 | 1 | 0 | 46 | 11 | 35 |
| **Self-Log** | 6 | 50 | 99 | 132 | 147 | 35 | 469 | 7 | 462 |
| **Self-Report** | 90 | 74 | 73 | 84 | 73 | 25 | 419 | 23 | 396 |
| **Spot Check** | 0 | 2 | 0 | 0 | 0 | 0 | 2 | 0 | 2 |
| **Totals** | **132** | **154** | **228** | **272** | **260** | **60** | **1106** | **59** | **1047** |

*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 noncompliance.

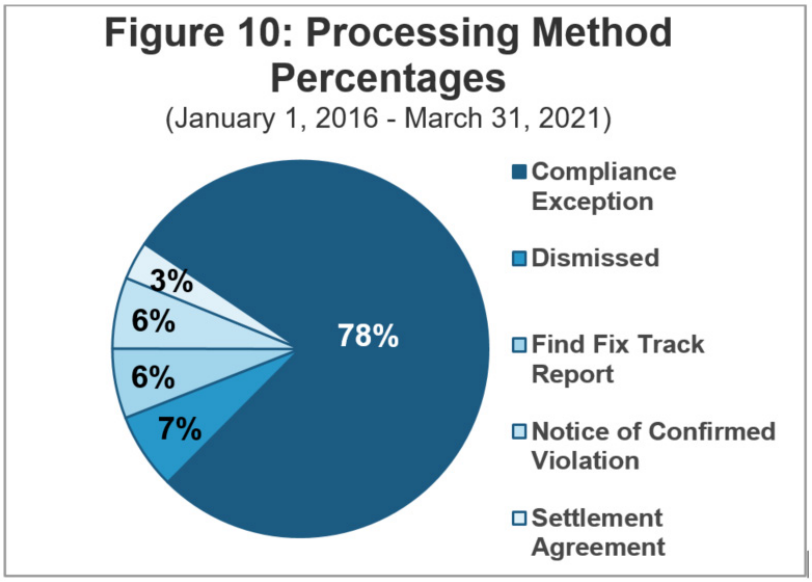



Figure 10 includes noncompliances for entities that were registered in the MRO region during the specified time periods.

*Noncompliance Processing Time (Figures 11 and 12)*

Figure 11 illustrates the trend of the average processing time for open instances of noncompliance reported to MRO before submission to NERC. MRO calculates the time based on the initial date MRO notifies NERC of the issue of noncompliance until the date MRO submits the instance to NERC for final processing or posting. The instances in 2016 were due to the transfer of a number of aged noncompliances to MRO from another member of the ERO Enterprise. Additionally, averages were also impacted with the increase of registered entities reporting to MRO starting in July 2018.

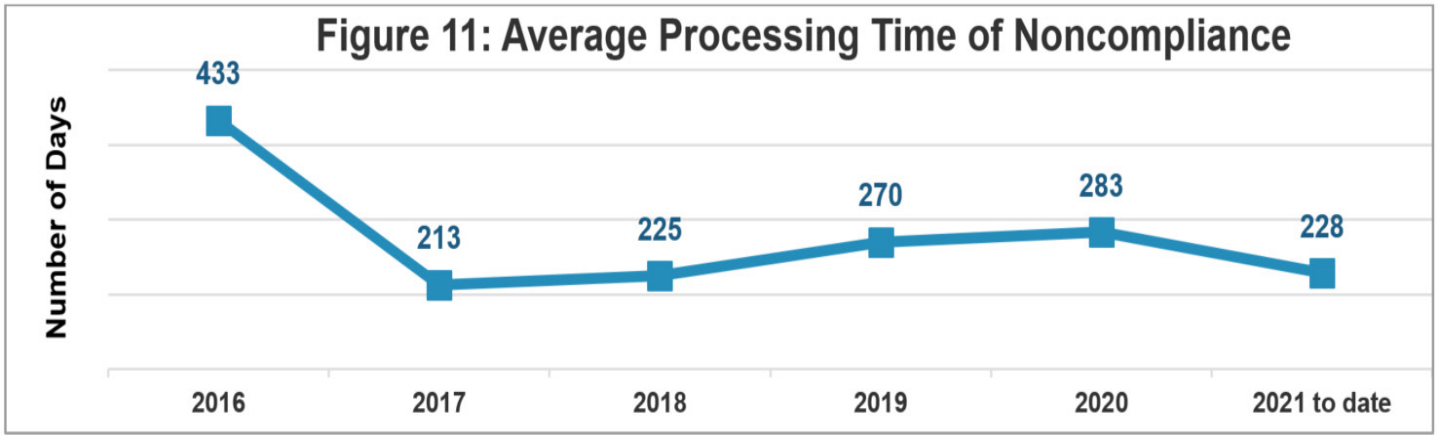
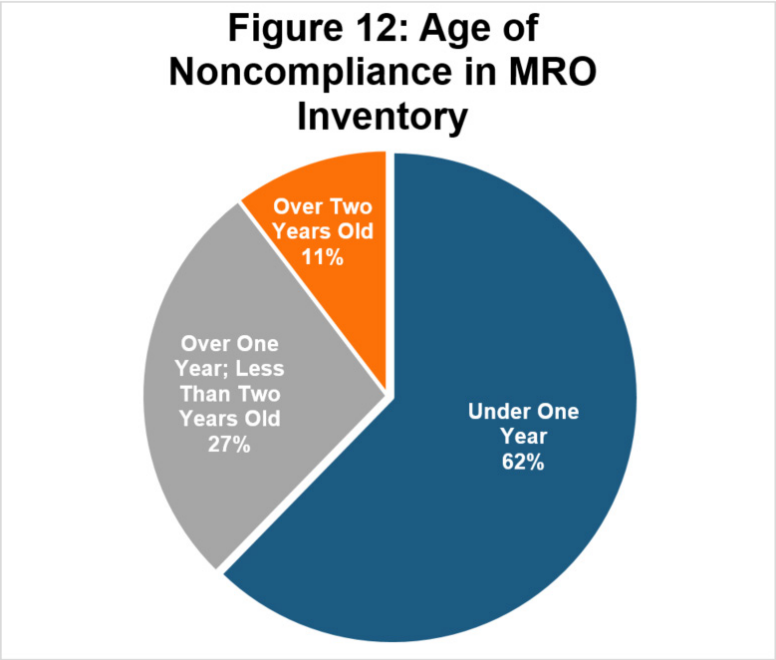


Figure 12 illustrates the trend of the average processing time for all open instances of noncompliance reported to MRO until they are fully closed and no further action is requested by the applicable government authority.




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

The MRO Compliance Department can be reached at compliance@mro.net

The MRO Risk Assessment & Mitigation Department can be reached at HEROS@mro.net

The MRO Enforcement Department can be reached at enforcement@mro.net

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

# Align and SEL Now Live!

We are excited to announce the Release 1 launch of the Align tool and the ERO Secure Evidence Locker (SEL), which has been live for MRO, NERC, and Texas RE since March 31, 2021. 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. If you have questions or problems concerning your ERO Portal account, please submit a support ticket here.

**Entities participating in the coordinated oversight program will go-live per the schedule of the assigned Lead Regional Entity (LRE).**

This initial launch marks an important milestone for the Align project, and the ERO will continue Release 1 deployment across the remaining Regional Entities between now and May 24, 2021.

Effective immediately, the functionalities listed below should be used in Align and the ERO SEL. However, the legacy application (webCDMS) should be used to continue processing any open findings already in the system. Please refer to the Registered Entity Start, Stop, Continue Guide for more details.

### Release 1 Functionality Overview for Registered Entity Staff

- Create and submit Self-Reports and Self-Logs
- Create and manage mitigating activities and Mitigation Plans
- Generate a report of standards and requirements applicable to your entity
- Receive notifications and view dashboards on open/action items
- Manage user access for your specific entity via the ERO Portal
- Receive and respond to Requests for Information
- View and track Open Enforcement Actions
- Submit evidence supporting the above processes via the ERO SEL

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 Regional Training Leads, Ryan McNamara and Michael Spangenberg at align@mro.net, with any 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*

# Version 5 CIP Evidence Request Tool

MRO has incorporated its customizations into version 5 of the CIP Evidence Request Tool (ERT). This customized version of the MRO ERT file is available on the MRO's website within the Audit Notification Packet Templates zip file. MRO will continue to communicate future updates through MRO's newsletter Midwest Reliability Matters.

For any additional questions or feedback about the baseline ERT or MRO's customized version, please feel free to contact elliot.weishaar@mro.net.

*- Elliot Weishaar, Compliance Engineer II, CIP*


# Joint Virtual 2021 CIP Workshop

## June 3, 2021 | 10:00 a.m. to 3:00 p.m. Central | Virtual Event

### Event Details

MRO is pleased to announce it will participate in a CIP Workshop hosted by Texas Reliability Entity on Thursday, June 3 from 10:00 a.m. to 3:00 p.m. Central. This fully virtual workshop will focus on **Supply Chain**, **CIP-012**, and **CIP-008-6**. Each topic will feature a presentation on compliance followed by a panel discussion of its security aspects. The presenters and panelists will consist of subject matter experts (SMEs) from across the ERO Enterprise, including representatives from:

- NERC
- E-ISAC
- ReliabilityFirst
- WECC
- MRO
- SERC
- NPCC
- Texas RE

### Registration

Registration is required for this event. Further details will be provided at a later date.

For questions, please contact information@texasre.org.

# REGISTRATION, CERTIFICATION AND STANDARDS

## Certification Reviews

All Balancing Authorities (BAs), Reliability Coordinators (RCs), and Transmission Operators (TOPs) registered in the NERC Compliance Registry are certified to perform respective functions. Certification verifies each of these registered entities have the tools, trained staff, processes, procedures, and the necessary cyber, and physical controls in place to meet the 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.

Each year, MRO publishes a reminder for any BAs, RCs, and TOPs experiencing a material change to its operations, 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.

On January 19, 2021, the Federal Energy Regulatory Commission (FERC) issued its Order of Five Year Compliance Filings, which includes modifications to NERC Rules of Procedure: Appendix 5A - Organization Registration and

Certification Manual. Among the modifications to Appendix 5A are the triggers for a certification review. A summary of the events that may trigger a certification review could be any of the changes listed below:

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

Of the three triggers precipitating a review, Modifications of the EMS experienced the greatest change. The previous trigger was the "complete replacement of an existing SCADA/EMS." Appendix 5A now states, "Modification of the Energy Management System (EMS) which is expected to materially affect CIP security perimeters or the System Operator's: 1) situational awareness tools, 2) functionality, or 3) machine interfaces." This in part, is in response to virtualization of the EMS.

To determine which modifications will require a review, MRO deployed a questionnaire to be completed by entities experiencing any changes. The addition of this questionnaire is consistent with other Regional Entities and is part of the ERO transformation project. The questionnaire will provide MRO a greater understanding of the scope of the change and its impact.

**"Of the three triggers for a certification review, modifications of the EMS experienced the greatest change."**

After review of the questionnaire, MRO may:

1) ask for further details, which may or may not, necessitate scheduling a review;
2) schedule a review;
3) 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, 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. 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 operations, or you have any questions related to a potential change in operations, please contact MRO at certification@mro.net.

*- Russel Mountjoy, Principal Reliability Specialist*

# BULK POWER SYSTEM RELIABILITY

*Photo by Anna Valberg on Unsplash*

## February Severe Cold Weather Event

Our entire industry is now very familiar with the severe cold weather event of February 15-17, 2021, and the impact that it had on the bulk power systems of several southern Midwestern states. During the second week of February 2021, meteorologists identified that severe cold weather from the upper Midwest would move southward into the southern Midwestern states by the following week. The states impacted most would be Texas and the southern states within the Southwest Power Pool (SPP) and Midcontinent ISO (MISO) footprints. Areas of southern Texas were expected to experience temperatures colder than what some parts of Alaska would experience. The forecast also indicated that the severe cold weather would likely arrive around February 14, 2021, and remain for three to four days.

The Electric Reliability Council of Texas (ERCOT) Interconnection in Texas was hit the hardest and required significant amounts of manual firm load shed for the better part of the three days, with limited ability to rotate the outages. This reduction in load was necessary to rebalance load with available generation, which was significantly lower than anticipated generation due to forced outages. A detailed presentation of what occurred on the ERCOT bulk power system during this event has been prepared by ERCOT staff and can be found here.

In the Eastern Interconnection, both SPP and MISO also experienced unusually severe cold temperatures in the southern portions of their systems. Both of these Regional Transmission Organizations (RTOs) also had to call for firm load shed within the RTO footprints, but the magnitude of load shed was much lower

than ERCOT's load shed requirements and the durations were fairly short. Several load serving entities also rotated outages when possible to minimize the impact to customers.

Reserve margins (the amount of expected generation available above forecast peak load) in winter are often projected as quite robust in many planning areas, as shown in the chart below taken from the NERC 2020/2021 Winter Assessment.

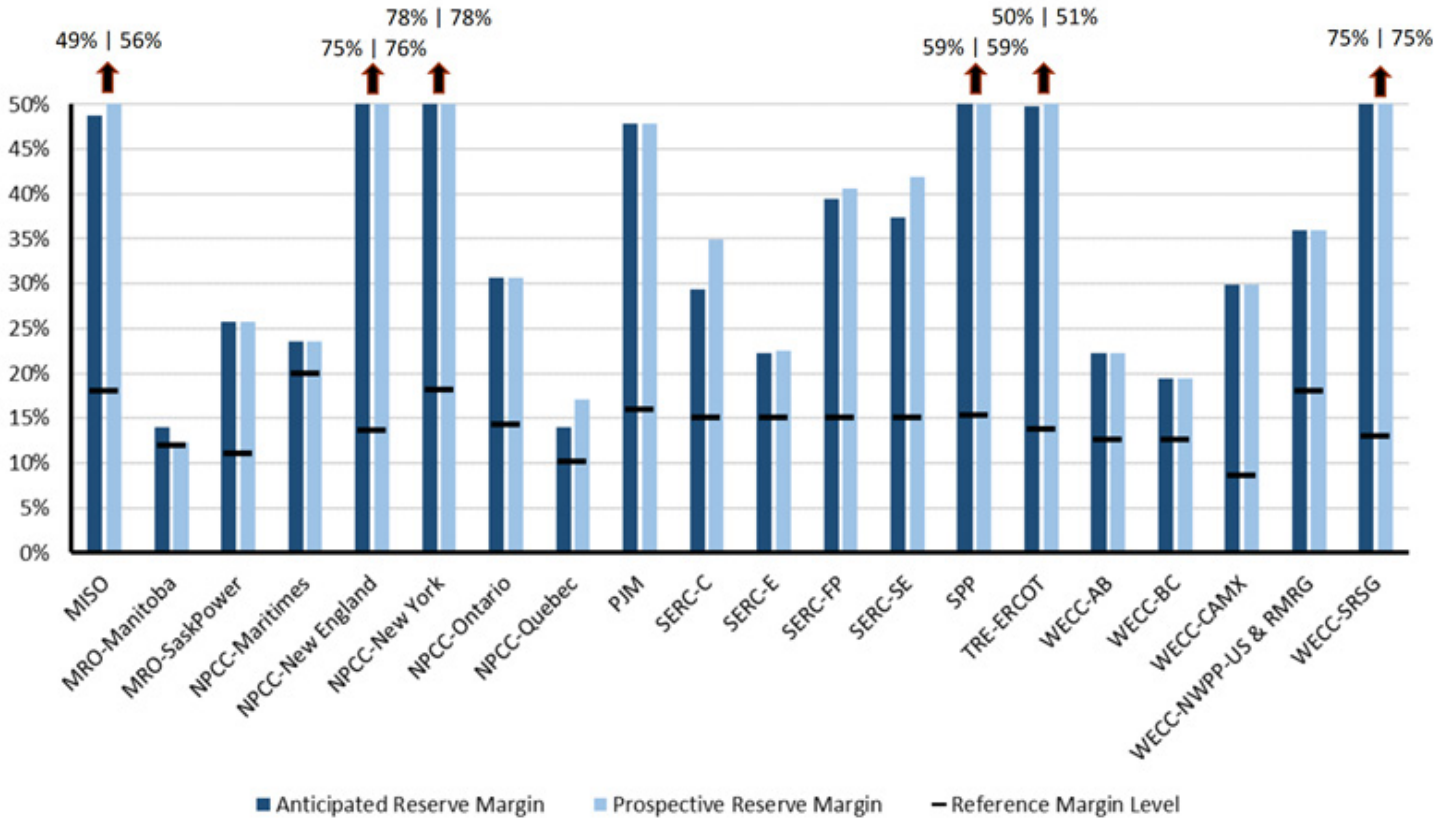
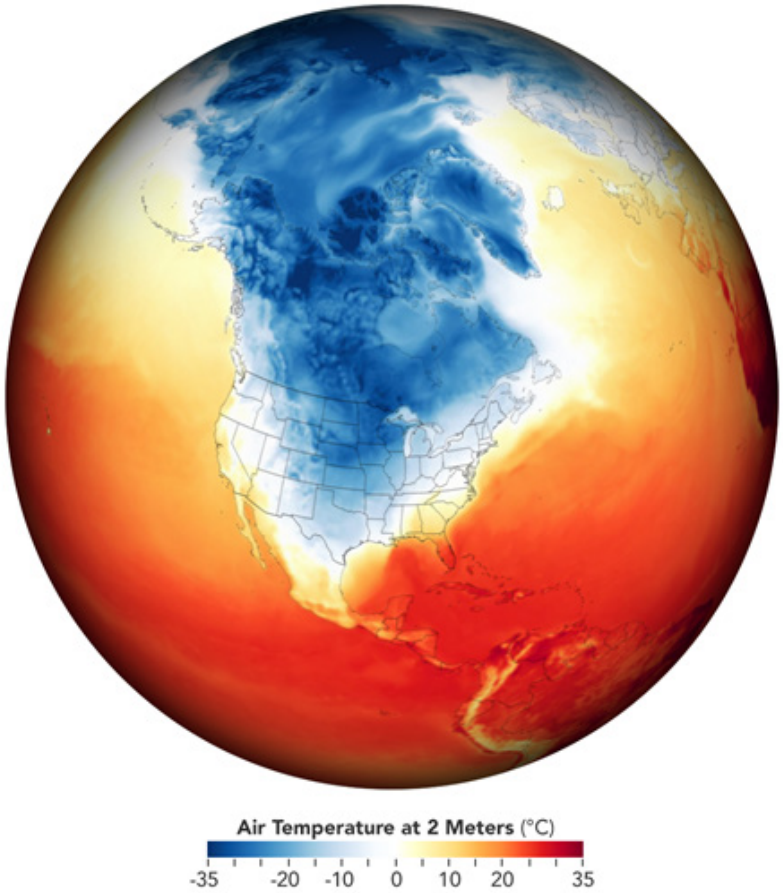



**Figure 2: Winter 2020–2021 Anticipated/Prospective Reserve Margins Compared to Reference Margin Level**

The MISO, SPP, and ERCOT anticipated reserve margins for winter 2020/21 are 49%, 59% and 50%, respectively. So how can severe cold temperatures reaching into the southern Midwest states cause such dire conditions that would ultimately result in emergency energy shortages and manual firm load shedding?

There were three key contributors:

- **Heating in the southern US is predominantly electric**. In the January 2018 severe cold weather event, one southern utility indicated that its winter peak 50/50 load forecast was based on an ambient temperature of +18° F. This entity's extreme load forecast (based on a 90/10 probability, or once in ten year event) was calculated using an ambient temperature of +13° F. This fairly minor 5° F difference in ambient temperature was identified to cause a 15% increase in winter peak demand on the entity's system, primarily due to electric heating load. It was also noted that the MW/degree relationship is not linear at these severe cold temperatures; the colder it gets, the MW of load increase per degree can be exponential.




*Source: https://earthobservatory.nasa.gov/images/147941/extreme-winter-weather-causes-us-blackouts*

- **A large percentage of generation in the southern Midwest uses natural gas as a fuel.** Roughly 60% of ERCOT's portfolio of generation is natural gas plants. A large percentage of these gas plants are not winterized for protection from sub-freezing temperatures. Many gas wells and gas supply equipment are also not winterized to protect against freezing. This caused gas plants to trip off line and gas supply to be compromised.

- **Wind generation in all three RTOs had very low production during February 15 to 17 due to lack of wind speed and lack of winterization of wind turbines**. The combined available wind generation nameplate for all three RTOs was about 69 GW for winter season 2020/2021. However, it was producing on average about 10-15% of nameplate during this three-day event, a reduction of roughly 60 GW from winter nameplate across the three RTOs.

The Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Corporation (NERC) opened a joint inquiry into the operations of the bulk power system during this extreme cold weather event. The Inquiry team will prepare a detailed event analysis report for both the ERCOT and Eastern Interconnections. Initial key findings are expected to be available sometime this fall. MRO staff members John Seidel and Russ Mountjoy are members of the Inquiry Team, along with staff from the Texas Reliability Entity, SERC Reliability Corporation, and ReliabilityFirst Regional Entities. MRO will work with others across the ERO Enterprise to provide industry with any key findings and recommendations once they are available.

*- By John Seidel, Principal Technical Advisor*

# Preparing for a Hybrid Future

The future electric generation resources in North America are going to be predominately inverter-based resources. Wind, solar, battery, and even hybrid interconnection requests can be seen in every major Transmission Service Provider's interconnection queues. With many corporations and utilities announcing carbon reduction goals, demand for these resources is simultaneously increasing.

The Inverter-Based Performance Working Group (IRPWG), formerly the Inverter-Based Performance Task Force, was created in the wake of the 2016 Blue Cut Fire Disturbance to investigate and make recommendations on system analysis, modeling, and performance of inverter-based resources under abnormal conditions. The group consists of representatives from transmission service providers, transmission owners, and generator equipment manufacturers. The top priority for the IRPWG was to develop performance, study, and modeling guidelines. Ideally, issues should be identified and mitigated before they can occur and having proper models, studies, and performance standards are vital to ensure ongoing reliability.

Recently, NERC published IRPWG's reliability guideline for Battery Energy Storage Systems (BESS) and Hybrid Plant Performance. This reliability guide includes a significant amount of information regarding hybrid power plant modeling. There are two types of hybrid power plant classifications discussed in this reliability

guideline; AC-coupled and DC-coupled. The distinction on pairing inverter-based resources on the AC or DC bus seems small, but that distinction does change the recommended modeling of the asset.

An AC-coupled hybrid is where each generator, such as solar photovoltaic, or wind is coupled with BESS and features its own set of inverters and will usually be coupled on the AC collector system voltage bus. Generally speaking, modeling of this type of hybrid would take into account each system explicitly using the recommended models for those generator systems.

Where modeling gets interesting is on the DC-coupled hybrids. In a DC-coupled system, the generators are basically sharing the same inverters. The recommended method for modeling is to have a single equivalent machine represent all the generators that comprise the hybrid facility. This is due to the fact that stability models represent the inverter in the simulation. In the case of a solar, battery hybrid, the recommended stability model would be the Renewable Energy Electrical Controller (REEC_C) model as this will most accurately capture the response of the system.

It is important to note that industry understands the capabilities needed to improve modeling hybrid power plants and the coordination of overall plant controllers. The next step is to develop recommendations for Electromagnetic Transient (EMT) models. These models are the most accurate representation for inverter-based resources, but their use and requirements vary widely amongst transmission service providers and planning coordinators.

*- David Brauch, Principal Engineer, MISO*

# About the Author

*David Brauch, Principal Engineer, MISO*

David Brauch is a Principal Engineer at Midcontinent Independent System Operator (MISO) performing Generator Interconnection studies. Prior to joining MISO, he was a Transmission Planning Engineer for Xcel Energy and served in the United State Marine Corps.

Brauch holds a bachelor's degree in Electrical Engineering from the University of Minnesota and a Master of Engineering Management from St. Cloud State University.

# Compliance with FERC Order No. 2222

The Federal Energy Regulatory Commission (FERC or Commission) issued Order No. 2222 in September 2020 (“Order” or Order 2222). In the Order, the Commission directed Regional Transmission Organizations and Independent System Operators (RTOs/ISOs) to modify their tariffs to remove barriers to the participation of Distributed Energy Resource Aggregators (“DERAs”) in (RTO/ISO) markets.

FERC defines a Distributed Energy Resource (“DER”) as any resource located on the distribution system, any subsystem thereof, or behind a customer meter. These resources may include, but are not limited to, electric storage resources, distributed generation, demand response, energy efficiency, thermal storage, and electric vehicles and their supply equipment. The Order is intended to be technology-neutral and covers all types of applicable resources – even those that might be invented in the future. Moreover, the Commission has required RTO/ISOs to permit heterogeneous DER aggregation, which may allow aggregators to group different technology types together.

DERA is defined as an entity that aggregates one or more DERs for purposes of participation in the capacity, energy and/or ancillary service markets of RTO/ISOs. Order 2222, like Order No. 841 before it, maintains the Relevant Electric Retail Regulatory Authority (RERRA) jurisdiction over its retail programs. As such, a RERRA is able to condition a DER’s participation in a retail program on that resource not also participating in the RTO/ISO markets. The Commission has also made the DERA the entity responsible for interacting with RTO/ISOs and other entities on behalf of its aggregated DERs.

## Summary of Compliance Requirements

The Commission has required RTO/ISOs to develop a holistic framework, including establishment of new market rules, to ensure communication and coordination amongst all affected parties such as the RTO/ISO, the DERA, the distribution utility, and the RERRA.

Some of the salient points are noted below:

- **New Market Participant Type**: RTO/ISOs must create as necessary, DERAs as a new market participant type.
- **Market Participation Agreements**: RTO/ISOs must revise tariffs to include a market participation agreement that defines a DERA’s roles and responsibilities and its relationship with the RTO/ISO. The agreement must include an attestation that the DERA is in full compliance with the tariffs and operating procedures of relevant distribution utilities and RERRAs.
- **Sizing Requirement**: RTO/ISO’s minimum size requirement for DERAs cannot exceed 100 kW. The Order doesn’t stipulate a maximum size requirement but defers to RTO/ISOs on whether any maximum size requirements should be established.
- **Information and Data Requirements**: DERAs must provide a list of individual aggregated resources and aggregate settlement data to RTO/ISOs. RTO/ISOs must also develop information sharing protocols to share necessary information with affected distribution utilities.

- **Metering and Telemetry Requirements**: It is up to the RTO/ISOs to determine how to satisfactorily address metering and telemetry hardware and software requirements, on the condition that such requirements do not pose undue barriers to individual DERs. RTO/ISOs must coordinate with distribution utilities and RERRAs to establish information-sharing protocols, as needed.

- **Locational Requirements**: RTO/ISOs are required to establish locational requirements for DERs to participate in a DER aggregation that are as geographically broad as technically feasible.

- **Distribution Factors and Bidding Parameters**: RTO/ISOs are required to establish market rules that address distribution factors and bidding parameters for DERAs.

- **Interconnections/Interconnection Studies**: In the Order, FERC declines to exercise its jurisdiction over interconnections of DER, deferring instead to the local interconnection process. It does not require RTO/ISOs to provide for standard interconnection procedures, agreements, or wholesale distribution tariffs. FERC has left the coordination with RERRA's and distribution utilities on interconnection studies and restudies up to the RTO/ISO's discretion.

## Impact on Reliability

The proliferation of DERs has been steadily increasing over the years and Order 2222 is only expected to give that a boost. RTO/ISOs are responsible for ensuring reliable and efficient operations of bulk electric systems. While they have adequate monitoring capabilities and situational awareness at the transmission level, which is essential in order to ensure reliability, RTO/ISOs have rather limited, if any, visibility on the distribution side.

**"The proliferation of DERs has been steadily increasing over the years and Order 2222 is only expected to give that a boost."**

Load-side resources such as demand response have participated in markets for a while and have helped ensure reliability by making additional capacity available, especially under emergency conditions. The penetration of these resources has been limited so far, such that detailed modeling of behavior is not crucial. However, as DER penetration increases to the point where it impacts flows on the transmission system, RTOs/ISOs will need to grapple with numerous reliability issues, some of which are noted below:

1. **Modeling**: Accurate modeling of distribution connected resources and aggregators is a foundational need from a planning, operations, and markets perspective, whether those resources participate in the wholesale markets or operate solely to modify retail load. Both reliability and economic modeling is critical to understanding DER impacts on reliable operations, as well as on future transmission infrastructure needs. With different technologies potentially integrated under a single DERA, modeling of the individual DERs and the DERA is crucial.

2. **Forecasting**: DERs are expected to change system operations due to increasing variability, uncertainty, and unconventional net load profiles. Higher DER penetration suggests increased real-time resource

variability as DERs react to local weather and load conditions. Accurate forecasting of DER and DERA behavior will thus be necessary to ensure reliable and efficient operations and infrastructure planning.

3. **Situational Awareness**: RTO/ISOs need to ensure adequate monitoring, situational awareness, and decision-making capabilities, even with high DER penetration. Communication and analytical capabilities (SCADA, ICCP, EMS, market systems, etc.) need to be developed to accurately visualize impact of DERs and ensure reliable operations.

### Going Forward

Each RTO/ISO must file tariff changes needed to implement the requirements of Order 2222 by July 2021. FERC will establish an effective date for the revised tariffs based on implementation dates proposed by the RTO/ISOs. Both SPP and MISO are engaged in extensive stakeholder discussions to navigate through the Order's implications and to chart out a path forward.

Given the complexity of the Order and the numerous stakeholders in both regions, MISO and SPP have each filed Motions for Extension of Time with FERC to move the filing date for compliance plans to April 2022.

The evolution of the electric system continues with the changing fuel mix and the introduction of new technologies. By leveling the playing field for distribution connected resources, FERC Order No. 2222 seeks to improve market efficiencies through increased innovation and competition.

*- Durgesh Manjure, Director, System Operations, MISO, and MRO Reliability Advisory Council Member*

## About the Author

*Durgesh Manjure, Director, System Operations, MISO*

Durgésh Manjure currently works as Director, System Operations at MISO Energy. He oversees the modeling services, regulatory readiness, and technical development teams that support the efficient and reliable operation of MISO's $22 billion energy market.

During his tenure at MISO he has held numerous positions in areas such as long-term transmission planning, generation interconnection, policy studies, operations and EMS engineering, and generation dispatch and balancing authority operations.

Durgésh has been actively involved in the industry with engagements at NERC, EPRI and IEEE. He is a Senior Member of the IEEE and holds BS, MS and Ph.D. degrees in Electrical Engineering.

# MRO Publishes Seasonal Assessment

In 2020, MRO published its first ever independent reliability assessment, the 2020 Regional Winter Assessment (2020 RWA). In 2021, MRO plans to publish both summer and winter assessments and will follow each up with a webinar highlighting the assessment and its findings. The webinar highlighting the 2020 RWA was held on January 26, 2021. The assessment is both a historical review of the 2019 winter season that identifies regional trends most impactful to system reliability, and an evaluation of resource transmission system adequacy necessary to meet projected winter or summer peak demands. The focus of the independent assessment is to utilize performance analysis data collected, such as the Generating Availability Data System (GADS), Transmission Availability Data System (TADS), and Misoperation Information Data Analysis System (MIDAS). The assessment also covers Bulk Electric System events by reviewing Event Analysis (EA) data from the previous year, at a high level. These events don't necessarily fall under NERC's Performance Analysis as they are reported and reviewed as they occur, rather than on a quarterly basis. This information is very important as it is the driver for lessons learned and identifying any meaningful trends that need to be corrected or mitigated.

As part of the assessment, significant Energy Emergency Alerts (EEAs) issued by Balancing Authorities are reviewed from the previous summer or winter seasons. The assessment also reviews the previous year's load forecast compared to the actual and provides an outlook on the upcoming season. Some of the detailed items under seasonal forecast include: projected resource mix, reported reserve margin for each Planning Coordinator (PC), projected peak demand and extreme low generation scenarios, and nameplate, as well as peak capacity wind. Key findings and what the focus for registered entities should be for the upcoming season are included in this assessment.

This assessment falls under MRO's strategic goal of Identification and Assessment of Emerging Reliability Risks, specifically in translating the impact of NERC Reliability Assessments. This independent assessment is not meant to replace the seasonal NERC assessments, but rather compliment them by focusing on the MRO region. Any feedback or suggestions is welcomed and encouraged. Comments can be submitted to reliabilityanalysis@mro.net

*- Bryan Clark, Director, Reliability Analysis*

# Industry Tips and Lessons Learned

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

- Controlled Islanding due to Wildfire Event
- Catastrophic Failure of 345 kV Oil Filled Metering Current Transformer in a Transmission Substation
- Battery Energy Storage System Cascading Thermal Runaway
- Transient Induced Misoperation: Approach II (Loss of Protection during Severe Weather Lightning)
- Transient Induced Misoperation: Approach I (Control Circuit Transient Misoperation of Microprossor)
- Root Cause Analysis Tools - Barrier Analysis
- Root Cause Analysis Tools - Change Analysis

EXTERNAL AND REGULATORY AFFAIRS

# State Regulatory Outreach Initiative

Happy spring, everyone. It is hard to believe it is already April! I am excited to bring External and Regulatory Affairs news to Midwest Reliability Matters. This section of the newsletter will include information on MRO's external affairs, along with news related to regulatory matters.

In 2020, MRO expanded its external affairs efforts and launched an initiative focused on building relationships with state regulators. This effort supports an ERO Enterprise outreach initiative to increase awareness and share information with state regulatory agencies to inform these individuals of publically available reliability and security information, and to enhance visibility into ERO Enterprise work.

MRO External Affairs and Reliability Analysis staff began meeting with state regulators within the MRO footprint in December 2020, following the release of NERC's Long-Term Reliability Assessment (LTRA). The purpose of these meetings is to provide details on how the grid is undergoing significant change that is unprecedented in both its transformational nature and rapid pace. MRO informed its members of this state outreach initiative and that MRO staff would be meeting with various state public utility commissioners and staff. To date, Bryan Clark, Director of Reliability Analysis, and I have met with commission staff from Kansas, Minnesota, Nebraska, and North Dakota. These initial 30 to 60 minute meetings provided commissioners and staff with information about MRO, including our vision and mission, a high-level overview of the ERO LTRA, and an opportunity to ask questions and provide topics of interest for future discussions. MRO also joined SERC Reliability Corporation in a meeting with commissioners and staff from the state of Arkansas, and ReliabilityFirst in a meeting with commissioners and staff from the state of Michigan.

Looking ahead, MRO External Affairs staff will maintain these relationships through periodic outreach on important assessments and reports, with the goal of becoming a trusted resource for information regarding bulk power system reliability and security. To kick off this initiative in 2021, Bryan Clark and I gave a presentation to the Nebraska Power Review Board on April 12. This presentation focused on who MRO is and what MRO does to protect the reliability and security of the grid.

# Regulatory Update

On January 21, 2021, President Biden appointed Richard Glick as Chairman of the Federal Energy Regulatory Commission (FERC). Glick joined FERC as a Commissioner in 2017. With the recent additions of Commissioners Allison Clements and Mark Christie, the five-member Commission is now fully staffed. The next open FERC Commission meeting will be held virtually on April 15, 2021, at 9:00 a.m. central. Information about the meeting can be found here.

On April 29, 2021, FERC is hosting a technical conference to discuss "Electrification and the Grid of the Future." The purpose of this technical conference is to begin dialog between the Commission and stakeholders to prepare for an increasingly "electrified future." Information about future FERC technical conferences can be found here.

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

*- Tasha Ward, Director of Enforcement and External Affairs*

SECURITY CORNER

# Return on Security Expenditure

## Concepts for Building a Business Case

With constantly evolving infrastructure security requirements and associated cost constraints, it's important to demonstrate the value of security protection measures. This newsletter article addresses basic elements found in a business case for strong security controls, whether it be cyber or physical security, and provides examples. The article is broken down into two sections, the first being high level elements of a physical security business case, and the second being an in depth examination of considerations related to cyber-specific threats.

### Business Case Development Methodology Considerations

- Understand key elements of developing infrastructure security requirements.
- Perform In-depth, on-going reviews of sometimes vague and elusive guidelines, standards, and mandates.
- Assess primary areas of security compliance, cross-referencing FERC, NERC, Executive Office, U.S. Department of Transportation Pipeline and Hazardous Materials Safety Administration, etc., mandates, orders and guidelines with current company standards.

- Assess current facility standards against requirements and develop new facility-based security standards.
- Submit all security related information for review by internal regulatory, tax, finance, legal, and operations groups to determine plan, timelines, and operational alignment.
- Research cost recovery alternatives (i.e., FERC or state PUC surcharges or new rate cases, bonus tax depreciation, cost mitigation factors, and cash flow).
- Develop project plans, obtain necessary approval, and assemble implementation team.
- Identify company assets in accordance with asset classification model.

Since we know we must do our part to protect critical infrastructure and realize that this goal is not inexpensive and perhaps comes during a difficult financial period, the elements listed herein are concepts to address security challenges based on risk. These concepts increasingly gain the needed support of other business unit leaders, as well as executive teams.

## Cost Mitigation Factors to consider

- Premium discounts for risk, cyber security and/or terrorism insurance
- Use of technology to reduce headcount and contractor staffing
- Use of shared services to reduce internal headcount or needed outsourcing
- Value-added services, using existing resources, to obtain a better return on expenditures

## Asset Classification Model Example

There are three levels of assets considered in this model:

1. *General Assets* – Those assets not requiring additional security based on redundancy or lack of interaction with grid.
2. *Key Assets* – Those assets demonstrating a significant risk to the corporation or not clearly defined (yet) as critical.
3. *Critical Assets* – Those assets that impact the reliability of the grid and may require security enhancements.

## Understanding Key Elements of the Infrastructure Security Requirements

Once you have identified the general, key, and critical assets of your facilities, then (and if applicable), demonstrate a regulatory mandate or industry standard that can be met or enhanced by implementing the recommended business case. Consider letting the mandates and guidelines speak for themselves and discuss them thoroughly in the shared education of your fellow business unit leaders and executive team.

## On-Going Review of Guidelines and Needed Resources

- Actively participate on national, regional (i.e. MRO Security Advisory Council), trade groups, and other state and local security and resiliency initiatives.
- Conduct legal research of requirements – assisted by your company's legal counsel and/or outside counsel.
- Implement cross-functional development team that includes staff from security, IT, HR, tax, regulatory, finance, operations, engineering, procurement and executive leadership.

- Communicate regularly with functional leaders and working groups to establish and apply an Asset Classification System to company facilities.
- Research, develop and validate security standards and alignment with security, operational, and compliance objectives.
- Benchmark security initiatives with multiple other utility companies.
- When appropriate, participate in selected meetings with state representatives and actively participate in the drafting of state legislation to support recovery.
- Revise master product and services agreements (using a "rule of 3") related to system integrators.

To help manage costs related to security expenditures, it is imperative to develop cross-functional teams to reduce overhead and improve return on investment.

Within the company, the resources needed to manage security projects may include legal, regulatory, procurement, IT, audit, facilities, tax, finance, operations, the executive team, and even third party vendors and strategic partners.

Benchmarking the success of security initiatives against other utility companies is also extremely important, especially with companies that closely resemble your organization's size and operations.

**"Benchmarking the success of security initiatives against other utility companies is also extremely important..."**

## Assess Primary Areas for Planning

- Force Protection – security officer support (as needed)
- Physical Security – lights, locks, barriers, cameras, visitor management
- Electronic Access Control – ID badging, intrusion detection systems (IDS) and duress alarms
- Cyber Security (Network and SCADA) - IDS, web filters, logical policy and process library development, vulnerability testing, forensic investigations, patch management, authentication & encryption and incident reporting
- Personnel Security – training and awareness, re-occurring background investigations, insider threat programs, clean desk procedures
- Incident Management - response, reporting and tracking
- Risk and vulnerability assessments of critical sites annually
- 100 percent annualized security awareness/response training for personnel of critical sites (In-person and web-based)
- Proprietary and non-public information protection
- Business continuity planning and testing

An interesting side note in reviewing the implications of new security enhancements is that they can literally affect every department, the entire employee population and a significant portion of your facilities (depending on their scope and operations).

It should also be noted that the site assessment methodology can start inside and work outward, and instead of stopping at the perimeter, continue for a radius of 1 to 3 miles around your facilities to identify things that

could readily impact your operations without penetrating your perimeters.

In conducting these assessments, an organization can rely on the basic elements of security:

- Deterrence
- Delay
- Detection
- Assessment
- Communications
- Response

## Determining Timelines & Resource Requirements

- Use of a project management tool with defined Work Breakout Structures and Timelines, Critical Milestones, Resources Availability and Resources Required
- Pre-Contract Order Negotiations with Multiple Technology Providers
- Development of Management Review Team and Operations Group with re-occurring meetings and as needed sub-Work Groups
- Favorable financial planning for recovery, tax depreciation and cash flow, combined with new procurement actions for fixed cost escalation strategy, proof of concept timeframes, AIA payment standards and a system commissioning & warranty program

## Things to Consider When Determining Financial Metrics

- **Total Cost of Ownership** = capital expenditures, direct resources, technical support, indirect infrastructure support and ongoing Operations and Maintenance costs.

- **Indirect Resources** = HR department, IT department, Employee Training costs/facilities, etc. NOTE: Indirect resources are often overlooked in calculating total cost of ownership and systems deployment and can add 10 to 15% to your project costs, whether using temporary support or backfilling of positions.

To be successful in today's challenging economic times, a utility Security Department may consider developing a "**Return on Expenditure**" (ROE) process.  A simple, yet effective formula is "positive financial metrics" /cost of security program = ROE.

## Positive Financial Metrics

Six possible methods of positive financial metrics include:

1. Percentage of the security costs in proportion to the overall value of the asset being protected (often less than 1%)
2. Risk and Cost Mitigation
3. Cost Distribution
4. Recovered Loss
5. Avoided Loss
6. Asset/Revenue Protection and Recovery

## Attempt to identify any “Value Added” opportunities!

In closing, it is sometimes possible to further demonstrate the security enhancement value by pursuing “value added” aspects such as:

- Partnering with the Operations groups for Lone Worker Safety support
- Assist with Traffic Flow Patterns and other Safety related issues
- Assist with supply storage and inventory, and other operations and maintenance support
- Partnering with Facilities and other functional groups for high pedestrian traffic areas, general population movement patterns, and other efficiency opportunities

## Drill down example - Framing DDOS Risk and Impacts to Utilities in Special Operational Conditions

What is the risk of DDOS to your utility? Each utility operation is unique with its own specific impacts related to DDOS, but when the risk is re-framed in special operational conditions like pandemic related operations, the management decisions can shift significantly.

## Example considerations to frame DDOS impacts on your utility:

- What is the threat: DDOS attack on Internet facing systems?
- What is the vulnerability: No technical mitigation for DDOS?
- Which asset or capability is at risk: Loss of access to human resources due to lack of remote work capabilities?
- What are the direct impacts?
- What are the indirect impacts?
- What is the exposure factor?
- What is the rate of occurrence?
- What is the single loss expectancy?
- What is the Annual loss expectancy?

The difficulty lies in the task of framing and re-framing the risk to create an understanding that is relevant to a new or altered operational reality like operating in a pandemic.

We know we are doing our best to protect the critical infrastructure, and we also know it is incumbent upon us to demonstrate the value of doing so!

*- John Breckenridge, Crisis Management/Insider Threat Program Manager, Evergy, SAC Vice Chair, and Michael Meason, Sr. Manager, Information and Security, Western Farmers Electric Cooperative, SAC Member*

# About the Authors

*John Breckenridge, Crisis Management Program Manager, Evergy*

John Breckenridge, CCP, is the Crisis Management Program Manager for Evergy based in Kansas City, Missouri. 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, he 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, he worked for six years in the Jackson County, Missouri 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, Breckenridge 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 he 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, and is a Licensed Private Investigator.

*Michael Meason, Senior Manager, Information and Security, Western Farmers Electric Cooperative*

Michael Meason, Senior Manager, Information and Security, was promoted to his current role in June 2018. He began his career at Western Farmers Electric Cooperative 11 years ago as a Senior Network Engineer and has also served as the Manager of Technical Services.

Meason has ten 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, operational technology (OT), telecommunications engineering, network engineering/operations, and cybersecurity.

Meason is an alumnus of Leadership Oklahoma Class 32.

# Supply Chain Compromise

## Potential risks to operational control systems

News of a new supply chain compromise affecting the SolarWinds Orion Platform was announced in December 2020. NERC distributed an Alert on December 22, 2020, with acknowledgement from registered entities required by midnight on December 24 and a response due by January 5, 2021. What is a supply chain compromise? Let's assess this threat.

A software supply chain compromise is malicious code, a back door intentionally left vulnerable, etc., embedded in software or a product from the vendor. Does it have to be software? No, it can be embedded in hardware as well. The compromise may be present when you purchase the product or could be added during a patch update or system upgrade. These types of compromises are difficult for users to identify and protect against.

The SolarWinds Orion product is an enterprise network management software. This is a product installed to monitor and manage multiple systems; thus, providing a valuable target for adversaries. Many administrators installed the software with high level privilege accounts. Once the initial compromise is made, the adversary can move across multiple systems. The compromise was developed by highly skilled, well-funded, and patient malicious actors who took great care in concealing their work.

In the case of SolarWinds, the malicious code was signed as valid by the vendor. The malicious actor was able to compromise the vendor's process to certify the code and make the malware appear to be legitimate. Unsuspecting customers, including many government entities, installed the product assuming it was safe. There are many sources of information on this compromise for the technical savvy individuals wanting to dig into the details.

It appears the objective of the compromise was to extract information based on observations of infected systems. The malicious attack, if left undetected for a longer period of time, may have escalated into further compromises. While the damage from the SolarWinds compromise is significant, this event is particularly troubling for those entities operating critical infrastructure. The SolarWinds compromise is a great example of the determination of some adversaries to attack our systems. Experience tells us this will not be the last. The important lesson to learn is that we are susceptible to attacks from malicious actors and we must be constantly on guard to identify threats and protect our systems. The NERC CIP Reliability Standards may have helped to limit the potential risk of a compromise to operational control systems in our industry.

As entities focused on protecting the bulk power system, it is important to realize that security requires a team effort from all involved. Vendors also need to protect their systems. The new CIP-013 Supply Chain Risk Management Reliability Standard is a step in the right direction. I like to say, we are on a journey with supply chain risk management and really just getting started on that journey. Will we solve this problem soon? It's highly doubtful. All of us should be constantly on guard for compromises. If something doesn't appear quite right, trust your senses and investigate the situation. Apply good business practices for security to operational and business systems.

*- Tony Eddleman, Director of NERC Reliability Compliance, Nebraska Public Power District, SAC Member*

# About the Author

*Tony Eddleman, Director of NERC Reliability Compliance, Nebraska Public Power Pool*

Tony Eddleman has been with NPPD since 1996 at the Doniphan Control Center. Working in various engineering and supervisory roles, he currently is NPPD's primary compliance contact for NERC Reliability Standards. Eddleman has been in this position since October 2009 and has successfully led the District through four on-site compliance audits (Operations & Planning and CIP). Prior to compliance, he worked as the System Control Technology Supervisor, where he managed the Energy Management System operation and completed two major upgrade projects. He led the District's efforts for the initial implementation of the CIP Cyber Security Standards. Eddleman started his career with NPPD as a Network Applications Engineer and served in that position for approximately three years. Prior to joining NPPD, he worked as an electrical design engineer, operations engineer, environmental engineer, and power plant operator in the United States Air Force. He retired from the Air Force at the rank of Major. He received a Bachelor of Electrical Engineering from Auburn University and is a licensed, professional electrical engineer in the states of Nebraska and Illinois.

Eddleman is the current chair of the NERC Supply Chain Working Group (SCWG) under the Reliability and Security Technical Committee (RSTC). He is a member of the MRO Security Advisory Council (SAC), the Southwest Power Pool (SPP) Reliability Compliance Advisory Group (RCAG), the Reliability Team of the Large Public Power Council (LPPC) and the North American Transmission Forum (NATF) Supply Chain Steering Team.

# STRATEGIC AND FINANCIAL UPDATE


## MRO Board Approves 2021 Corporate Goals and Metrics

In the first quarter of 2021, MRO staff focused on developing annual corporate goals and metrics to support MRO's Strategic Plan and Operating Objectives. The six priorities of that plan are:

1. Maintain risk-responsive Reliability Standards
2. Strengthen objective risk-informed entity registration, compliance monitoring, mitigation and enforcement
3. Reduce known reliability risks
4. Identify and assess emerging reliability risks
5. Identify and reduce cyber and physical security risks
6. Improve effectiveness and efficiency

At its March 25, 2021 meeting, the MRO Board of Directors approved the 2021 Corporate Goals and Metrics.

There are a number of goals that relate directly to risks prioritized in MRO's 2021 Regional Risk Assessment (2021 RRA).

Uncertainty of planning reserve margins is one of the top risks identified in the 2021 RRA, and has been a contributing factor to impactful events within the region over recent years. This was perhaps most notable this February, when severe cold weather caused operators in the Eastern and Texas Interconnections to shed firm load when reserve margins shifted to negative values due in part to the unavailability of generation. John Seidel's article in this issue provides more insight into this recent event. In 2021, MRO staff will actively participate in the FERC-led inquiry into this event in order to determine lessons learned and additional actions that should be taken to prevent such future events. Additionally, MRO hopes to begin generation site visits under its new generator cold weather preparedness program.

Last year, WECC and NERC conducted analysis of models associated with inverter-connected resources, focused on solar assets. The results of that analysis identified the need for improvements in those models to support the ability to study the system as it undergoes a transformation, and to make sure operators are provided with sufficient information regarding generation resources to operate the system, as well as ensure adequate reserve margins. In 2021, MRO plans to work with NERC on a similar initiative focused on wind assets. The MRO region has more wind assets than any other region and the need for accurate models and awareness of ride-through capability of these assets within our region is of paramount importance in ensuring operators have sufficient awareness of wind resources, particularly on challenging days when reserve margins are low.Because MRO has these types of unique attributes, we will follow up on our 2020 first ever regionally-focused assessment by producing two MRO regional assessments focused on generation adequacy—one for winter and one for summer, and will conduct outreach on the results.

In addition to these regional assessments, MRO plans to further mature its Regional Risk Assessment report by incorporating industry into the ranking of security and reliability risks, utilizing volunteers from our three advisory councils. The 2021 RRA was the first year MRO ranked risks utilizing the MRO Reliability Risk Matrix, an idea that came from MRO Reliability Advisory Council Dallas Rowley. This tool has been revised based on input from MRO staff, the MRO Board's Organizational Group Oversight Committee (OGOC), and all three of the Advisory Councils. MRO is now working with partners across the ERO Enterprise to evaluate the opportunity to use this tool ERO-wide, to allow for more comparable assessments across the Regional Entities and by NERC's technical committees.

Other major focus areas for us in 2021 include implementation of the Align and the Secure Evidence Locker tools, continued outreach through our organizational groups, and a number of corporate intiatives focused on effectiviness and efficiency. These effectiveness and efficiency iniatives include individual development plans for all staff, a corporate Enterprise Risk Management Program, maturation of our diversity and inclusion efforts, and aligning our emergency response plans with the ERO Enterprise where appropriate.

I encourage you to reach out to me if you have any ideas or want to contribute to these initiatives. As a reminder, most of MRO's organizational group meetings are open to the public, and we encourage participation. 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:

### FERC Addresses Demand Response Opt-Out for Certain DER Aggregations

The Federal Energy Regulatory Commission (FERC) took additional steps on March 18, 2021, to break down barriers to the participation of distributed energy resources (DER) in wholesale markets by ensuring that demand response resources can combine with other forms of DERs to benefit consumers, enhance competition and promote grid reliability. See the full announcement.

### FERC Clarifies Determination of 80-MW Capacity Cap for QFs

On March 18, 2021, FERC reversed a split decision in a September 2020 order denying Broadview Solar LLC's application for certification as a qualifying facility (QF) under the Public Utility Regulatory Policies Act (PURPA). The Commission reinstated its longstanding "send-out" analysis, which determines a facility's power production capacity based on the electricity that it can actually deliver to the interconnecting electric utility. See the full announcement.

### FERC Announces Technical Conference to Discuss the Resource Adequacy Developments in the Western Interconnection

The purpose of this conference on June 23-24, 2021, is to discuss resource adequacy developments in the Western Interconnection. The Commission seeks to engage varied regional perspectives to discuss challenges, trends, and possible ways to continue to ensure resource adequacy in the Western Interconnection. See the event details on FERC's website.

### FERC Issues Supplemental Notice Inviting Comments on the Technical Conference Discussing Climate Change, Extreme Weather, & Electric System Reliability

On June 1, 2021, FERC staff will convene a technical conference to address concerns that because extreme weather events are increasing in frequency, intensity, geographic expanse, and duration, the number and severity of weather-induced events in the electric power industry may also increase. See the event details on FERC's website.

### NERC Calls for Abstracts for GridSecCon 2021

NERC is looking for physical and cyber security best practices and the challenges facing the industry from grid security professionals. Submissions are welcome from asset owners and operators in physical or cyber security roles, academic researchers, and industry and government experts. Training sessions will be in four hour increments; breakout sessions will be in one hour increments. Submit an abstract for a training or breakout session topic by April 21. Successful submissions will be notified by May 17. For more information or assistance, please contact events@eisac.com.

### NPCC Appoints Charles Dickerson as New President and CEO

The Northeast Power Coordinating Council, Inc. (NPCC) is pleased to announce the appointment of Charles Dickerson to succeed Edward A. Schwerdt as NPCC's president and CEO. Dickerson will assume his responsibilities on March 8, 2021. Read the full announcement.

## INDUSTRY EVENTS:

### Industry Webinar: Project 2019-06 Cold Weather

**April 14, 2021 | 1:00 to 2:00 p.m. Eastern**

The Project 2019-06 Cold Weather standards drafting team will provide an overview of modifications made to the second draft of the EOP-011, IRO-010, and TOP-003 standards and associated implementation plan. A question and answer session will be held following the presentation. Register here.

### ndustry Webinar: NERC Energy Management System Performance Special Assessment (2018-2019)

**April 28, 2021 | 2:00 to 3:00 p.m. Eastern**

The purpose of this special assessment is to gain a

better understanding of the contributions of energy management system (EMS) outages to the loss of situational awareness reliability risk, and the potential impact EOP-004-4 is having on situational awareness reporting for qualified/defined events in the ERO Event Analysis Process. This document includes assessments for outage duration, EMS functions, and entity reliability functions and examines associated trends identified for the 2018–2019 period. NERC will conduct a webinar to provide an overview of the special assessment. A Q&A session will follow the presentation. Register here.

### Save the Date for NERC's Human Performance in Electric Power Virtual Sessions

**May 6, 2021 | 1:00 to 5:00 p.m. Eastern**

Please save the date for the first session of NERC's Human Performance in Electric Power virtual sessions. This collaboration between the Electric Reliability Organization Enterprise, the Human Performance Community of Practice (KnowledgeVine and ResilientGrid) and their mutual partners brings together industry representatives and subject matter experts from across the country to share ideas and transfer knowledge about human performance topics/principles and their application in electric power organizations. More information will be available on NERC's calendar.

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

**May 12-13, 2021 (by WebEx)**

In response to ongoing COVID-19 developments, many utilities and organizations' travel restrictions are still in place to protect the health of their workforce. Based on this, NERC's Board of Trustees and the Member Representatives Committee leadership decided to convert all NERC 2021 2nd Quarter meetings to teleconference/WebEx. See the schedule of events or register for the board meetings 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.

## REGIONAL AND MRO EVENTS:

### Industry Webinar: Unmanned Aircraft System Security Threats and Mitigations

**April 29, 2021 | 9:15 a.m. - 10:15 a.m. Central**

MRO's Security Advisory Council (SAC) is pleased to announce it is hosting a webinar on Unmanned Aircraft System Security Threats and Mitigations. The SAC will be joined by Sarah Jacob from the Cybersecurity and Infrastructure Security Agency (CISA). Read more and register here.

### MRO CMEP Advisory Council Monthly Call

**May 11, 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 Protective Relay Subgroup Meeting

**May 25, 2021 | 8:00 a.m. to 4:00 p.m. Central**

The Protective Relay Subgroup will meet by WebEx on May 25 at 8:00 a.m. Central. 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