“The secret of change is to focus all your energy not on fighting the old, but on building the new.”

-Socrates
Inside This Issue

3  CEO Message

6  Corporate Values

8  Compliance Monitoring and Enforcement Program

22 Registration, Certification and Standards

25 Bulk Power System Reliability

26 Tips and Lessons Learned

31 Security Corner

36 MRO Interviews the E-ISAC

43 Strategic Update

45 Industry News and Events
MRO has undoubtedly undergone a transformation over the past couple of years. We expanded our footprint and doubled the number of registered entities in our region, increased staff such that more than 50 percent have been with the company two years or less, and made several governance changes, including reworking our organizational group structure and increasing the size of our board (notably 14 of 23 directors joined in 2019 or 2020). On top of all of these changes, we (like many others in the industry) transitioned to fully remote work for much longer than anyone would have predicted as a result of the COVID-19 pandemic. All of these changes have happened in my short tenure as President and CEO. Late June marked my two year anniversary serving in this role, and as I reflect back on all that has happened during this time, I find myself wondering, “What does it mean to be a fearless leader?”

In considering this question, I happened upon the website www.leadfearlessly.com, which describes fearless leaders as those that embrace change, influence and motivate others to become more fearless, to be open to change, and to grow and adapt. It is fearlessness that allows leaders to not only embrace change, but to learn from it and try new approaches if something does not succeed, Rather than being paralyzed by
uncertainty, fearless leaders learn from mistakes and create change for the better. To do so takes boldness, courage, persistence, and faith. All of these characteristics add up to fearlessness.

Fearlessness is a trait I see evident across the industry that we serve. Changes in the industry are occurring on multiple dimensions and happening very rapidly, whether it’s the changing generation resource mix, use of batteries and other devices within the distribution system, rapidly evolving security risks, cross sector interdependencies, or blurring jurisdictional boundaries. This rapid pace of change results in new and evolving risks to reliability and security of the bulk power system, and it takes a certain amount of fearlessness to adapt and create change for the better.

As a technical regulator, MRO recognizes that it takes a village to manage risk. Industry stakeholders are critical to ensuring risks to reliability and security are identified, prioritized, and mitigated. MRO’s three advisory councils are comprised of industry experts who are tasked with doing just that. For example, at the start of the pandemic the Security Advisory Council’s weekly Threat Forum quickly implemented a separate weekly call for entities to share information on the pandemic, along with planning, response, and mitigation strategies. The Reliability Advisory Council continues its important work to assess regional power system events and mitigate the primary drivers of those events, such as misoperations, and is also working on a tool to prioritize risk. The CMEP Advisory Council and its subgroups review and discuss new or revised Reliability Standards, develop application guidance on the standards when necessary, and share best practices related to compliance programs across the region.

All three councils provide input to and help develop MRO’s Regional Risk Assessment that is published annually, and provide a significant amount of outreach to regional participants. As you can see, involvement of industry stakeholders is an important component to the success of virtually every initiative we have undertaken at MRO over the years, and continues to ring true today.

Another important change that is influencing our work at MRO is the transformation that has been occurring across the ERO Enterprise—this is the term for NERC and the Regional Entities, collectively. Back in December 2018, Jim Robb, President and CEO of NERC, brought the Regional Entity CEOs together to discuss the unique opportunity that presented itself to “re-boot” the ERO Enterprise, recognizing the restructuring of the regional footprints in the Eastern Interconnection, the emergence of new leaders at NERC and in many of the Regional Entities, and an opportunity to create new and different ways to provide value. Transforming how we work together to support our shared vision and mission, improve our performance, and provide value, is a necessary first step in optimizing the brilliant ERO model.

Working collectively across the ERO Enterprise, we can learn from and leverage the expertise and innovation that exists outside the MRO region. We can create synergies by working more collaboratively with our colleagues at NERC and the other Regions. This benefits the entire ERO eco-system, as registered entities are better served by more informed and collaborative decision-making, providing deference to expertise as appropriate.

Throughout this reflection of the changes MRO has undergone in the recent past, and the efforts underway to transform the way we work across the ERO Enterprise, I am reminded that change is constant, and transformation requires a conscious choice. What we are experiencing today is a fearless approach to embracing change, with a conscious choice and commitment to work together to achieve success in ensuring reliability and security of the North American bulk power system.

Together, our future is bright!

-Sara Patrick, MRO President and CEO
Employee Spotlight

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

Amie Johnson joined MRO in June as a Business Analyst. She has over seven years of experience in the BA role working with business end-users to define and document business requirements, writing and coordinating end user testing, and building SharePoint sites. Her knowledge and prior experience in these areas will be a great addition to our team.

Cassandra Barbato accepted the position of Meeting Planner in July, and will oversee all of MRO’s meetings and events. She has a Hospitality Management degree and brings with her several years of experience working in the hospitality industry, most recently with Radisson Blu. We look forward to the improvements she will undoubtably make to our on-site event processes, and also to her help converting our planned onsite events to a virtual environment during the pandemic.

Recent Promotions:
Mark Flanary accepted the position of Manager of Risk Assessment and Mitigation, CIP. Along with his experience at MRO, Mark brings years of experience managing engineers (and customers) in the delivery and support of large Energy Management Systems. We look forward to the wealth of knowledge he brings to his expanded role.

New Diversity and Inclusion Committee:
The following employees were appointed, out of the many that volunteered, to MRO’s new Diversity and Inclusion Committee:

• Alexis Larson
• Rumyana Kreidler
• Rich Samec
• Holly Haynes
• Max Desruisseaux
• Julie Sikes

Read more about the work of this committee in the following article on “Equity, Diversity, and Inclusion” on page 6.

MRO is hiring! The following positions are posted on the Careers Page of our website:

• Risk Assessment and Mitigation Engineer, Operations and Planning
• Senior Power System Engineer (Compliance Monitoring Engineer/Auditor, Ops & Planning)

Watch our Why Work For MRO video to learn more about us. To apply, visit the on our website or visit us on LinkedIn.
Equity, Diversity, and Inclusion

Foundational values or hollow phrases?

Diversity and inclusion have been important foundational values within MRO, and we have a solid history of putting those concepts to action with the approaches we’ve taken to staffing and running the organization. However, in the recent unrest following George Floyd’s death, there has been a heightened awareness of the areas in which more can be done, and an introspective look at the organization revealed a shared desire to form a team dedicated to these important issues. This notion was highlighted by the following comments Sara Patrick, President & CEO, shared with MRO employees on June 10, 2020, about how we all can and must do better. “The horrific and eye-opening events surrounding George Floyd’s death call for us to condemn injustice and discrimination and reaffirm our commitment to live by our values and continue to cultivate a workplace that makes equality, diversity, and openness priorities. There is no better time than now to exercise curiosity, educate ourselves, and learn how we can be better together.” She announced the formation of a new Diversity and Inclusion Committee made up of staff volunteers to assess ways in which MRO could be more diverse and inclusive.

Inclusion in the workplace can be described as a collaborative, supportive, and respectful environment that encourages and embraces the participation and contributions of all employees. Although it’s easy to say that we all embrace this concept, the unfortunate reality is that inclusion isn’t always exhibited in practice. It may not even be a conscious oversight, but the barriers that often exist or develop within the workplace can lead to a “silent” discrimination or intolerance that ultimately results in the culture not matching how a company defines itself.

Workplace diversity is understanding, accepting, and valuing the differences everyone brings with them. It can include race, ethnicity, gender, age, religion, disability, sexual orientation; and it can also include education, personalities, skill sets, experiences, and knowledge bases.
History books and our own personal experience can identify times in this country during which there has been broad outrage about inequality and calls for our workplaces and society to be more inclusive. The recent events that have again brought this topic to the forefront follow a similar pattern; however, this time it feels different. Perhaps it is because the pandemic has affected the global population and has resulted in unprecedented changes in everyone’s life. Society has been forced to view routine tasks and functions through a new lens, and we might find ourselves asking why we perform tasks a certain way and if there is a healthier and more effective way to do so. It’s through this lens of reevaluating workflow that we can also reevaluate the workplace as a whole, and how we connect and work with each other.

The events that have taken place locally, regionally, nationally, and internationally provide clear examples of where equity, diversity, and inclusion have been absent or nothing more than hollow phrases. Organizations, including MRO, can seize this moment to shine the light on what is or isn’t happening within the workplace. Are we attracting, recruiting, and retaining with a focus on diversity, or do we tend to focus on like-minded and familiar backgrounds? Do we approach decisions and practices that apply fairness and equality? Are we creating an environment where employees feel comfortable speaking up and sharing differing experiences and opinions?

Diversity and inclusion are certainly not new concepts, and organizations such as MRO are moving in the right direction by forming dedicated teams of employees to focus on the topic. There is much to be gained by providing employees an opportunity to “have a seat at the table” and to voice their ideas or concerns in a respectful manner without hesitation or fear of retaliation. Even if a group such as this doesn’t produce sweeping organizational changes, it would be a mistake to discount the value gained by each participant becoming more educated on the differences and similarities of their fellow coworkers. The power of conversation and the sharing of ideas can produce lasting changes that are more valuable to the corporate culture than policies and procedures.

We want all MRO employees to feel valued for their skills, talent, and the work that they perform. Equally as important, we want all MRO employees to feel valued for the uniqueness they bring to the organization. Can you imagine how dull and boring the company would be if we were all a carbon copy of one another? It’s no surprise that studies have shown that the more diverse a workplace is, the more success it achieves.

Interestingly, Deloitte published the results of a 2015 study titled, “The Radical Transformation of Diversity and Inclusion: The Millennial Influence.” This study found that workplace diversity is defined and perceived differently by generations. Millennials tend to combine different backgrounds, experiences, and personalities and believe that it is these differences that ultimately lead to innovation. The Generation X and Baby Boomers view workplace diversity demographics as applying equality and fairness to all employees. Understanding and accepting these types of differences in interpretation is just one of the ways inclusion can be fostered within an organization.

It is with an eye to the present and the future that MRO will be hosting an all-staff training related to recognizing and understanding Unconscious Bias. We look forward to this upcoming event sponsored by the new Diversity and Inclusion Committee, and we will continue to look to the committee to identify opportunities related to diversity, equality, and inclusion to make MRO a better place for all of us by obtaining input and learning from each other.

-Karla Schiller, Director of Human Resources
Our industry shares one primary objective: the safe, effective, reliable operation of the Bulk Electric System.

NERC Reliability Standards set minimum criterion for operations, planning, and security to provide assurance that our primary objective can be met. The standards do not, however, define the expectation for an internal assurance program; entities may rely solely on external oversight by their regulator(s) for that assurance.

In this article we discuss how an entity can leverage governance models such as the three lines of defense and internal independent resources to take their assurance to the next level, while reducing dependence on external regulatory oversight. This internal layer of assurance can provide significant benefits in the form of cross functional collaboration, transparency, and effective risk management.

We all know too well that being compliant and demonstrating compliance are two different things. Many of us are no stranger to industry best practices and have been operating in that way for as long as we can remember. We’ve also learned over time that for best practices to be effective, sustainable, and repeatable, we must document them. However, we realize that documented processes alone rely on subject matter experts adhering to that documented process.

Without verification, any entity is left to assume that processes are designed effectively, operating as designed, and procedures are being executed as written. Without self-assessment, how would you know? And how can you be certain that you have identified and mitigated all potential gaps? Ah, there it is! The next layer of risk management is born, and who is best to help an organization provide independent objective assurance than the third line of defense; your Internal Audit department?

The Internal Audit
Partner or patrol officer?
The natural response to this approach being, “Wait. What? Come on, you know I have limited resources. Now you want to impose an internal audit, too?” For many organizations this is an uncomfortable notion: a perception that Internal Audit only gets involved when someone screwed up, or someone thinks that you aren’t doing your job. At this point, it would seem human nature to think that an Internal Audit team is only digging for issues and that each internal audit places a target on a ‘problem.’

**Reliable operations mandate a change in mindset.**

When a member of Internal Audit walks by or calls, do you cringe and say, “Oh no, what did I do wrong now?” Or do you welcome the engagement and ask, “How can I leverage the Internal Audit team to reduce risk and exposure for my organization?” The answer lies in your perspective about the Internal Audit function and its objectives. **Ask yourself, is Internal Audit my business partner or patrol officer?**

Most Internal Audit teams are not out on patrol, walking the hallways, monitoring your every action, just waiting to swing by and judge you, charge you with a ‘ticket’ if you don’t perform each and every step in your compliance process related to compliance requirements. Instead, they are curious and experienced risk practitioners that want to learn your process and contribute a fresh perspective to help focus on mitigating risk for your department and organization.

The reaction to an auditor reviewing and validating someone’s work can be all too common, “Hey, I’m doing all I can. I am qualified for the work, and I do the right thing. You want to verify my work? So, wait, you don’t trust me to do my job?”

For many of us operating in an oversight role, this response is all too familiar: “Wait, did you say that I need to do even more? I have limited resources – people, time, budget! I am already redirecting resources to do these ‘extra’ compliance tasks, to monitor and respond to the changing regulatory environment, to implement new or revised standards, all while doing their day-to-day tasks – I cannot possibly add another piece.”

**A business partner adds value beyond merely policing non-compliance**

Internal Audit does more than protect the company and its assets by assuring what is implemented is working effectively; they can be viewed as a partner that fosters continuous improvement and process maturity for the organization. Internal Audit also can provide consultative services and value enhancement, and you should leverage them as another resource in value optimization.

And, is it just Internal Audit, or is there a partnership opportunity between your Compliance and Internal Audit teams? Do you have segregation of duties between the second and third lines of defense, or is one of these teams performing both tasks without that independent perspective?

An entity’s strategy and approach to governance, risk, and controls can be the difference between being good and being lucky—or as we noted above—between “being compliant” and “demonstrating compliance.” At the end of the day, every employee shares a common interest to do right by their company to assure the safe, effective, **reliable** operation of the Bulk Electric System. Having a “One Team” approach can break down artificial silos to work together rather than against one another. When it comes to compliance with the NERC Reliability Standards, no matter the registered entity, internal relationships are key, especially with the Internal Audit department.

Internal Audit should recognize how its role can be perceived by its internal clients and how to invest time to build credibility and rapport in the relationship. Being approachable is key, and when internal clients view internal audit as a trusted partner, they come to recognize Internal Audit as an extension of their team sharing a common goal with all involved to achieve and maintain success.
Everyone shares the responsibility to keep a conversational non-adversarial tone, and to assure Internal Audit engagements are opportunities to learn and improve. When everyone is interested in each other’s success, feedback becomes a gift, and everyone involved shares the reward.

Is this shift in mindset easy? No, admittedly not. But the potential value from partnering with experienced Internal Auditors is high, even if it requires upfront work and uncomfortable conversations. So, the next time you see Internal Audit on the caller ID, just remind yourself: Partner or Patrol Officer, the choice is yours.

-Co-authored by Sharon Koller and Benny Akowuah, American Transmission Company. Sharon is a member of the CMEP Advisory Council.

About the Authors

Sharon Koller, Reliability Standards Compliance Strategist & Assurance Manager, joined ATC in 2013 with 23+ years’ experience in the utility industry. Koller is focused on contributing to safe, resilient, and reliable operation of the BES through implementation of sound security practices and internal controls. Koller serves as ATC’s CIP Senior Manager in an internal assurance, oversight, and governance role providing CIP interpretation and advisory services; management of potential non-compliance; operational alignment of centralized programs, metrics, and tools with ATC’s reliability and security strategy. Koller is a member of the 2016-02, 2019-02, and 2019-03 CIP Standards Drafting Teams, and serves as an MRO CMEP Advisory Council member.

Prior to ATC, Koller served Alliant Energy for 16 years, in various technical, compliance, project, and program management capacities.

Bernard (Benny) Akowuah, CISA, CGEIT, CRISC & CDPSE has spent the last 4+ years with American Transmission Company. He is responsible for executing risk assessment of NERC Reliability Standards and Business Impact Assessment (BIA), developing and managing of Internal Controls, assurance and compliance activities, designing and implementing policies and standards, and contributor to Enterprises Risk Management and Business Continuity Management.

Benny has 19 years of experience in auditing, risk management, governance, compliance, internal controls and Information Technology.
Status of Align Tool Release

The Align Tool is a culmination of strategic efforts that began in 2014 with the goal of improving and standardizing processes across the ERO Enterprise. Align will be released in three phases, with the first phase scheduled to roll out in Quarter 1 of 2021 with MRO and Texas RE being the pilot regions. The first phase will include Self-Reports, Self-Logs, and all Potential Non-Compliance processing and associated mitigation work.

Each region within the ERO Enterprise recently held testing with a select number of entities within their region. MRO selected three entities: Evergy, Oklahoma Municipal Power Authority, and Xcel Energy, to test the functionality of different work flows of multiple scenarios within Align. MRO will hold a follow-up testing session in August with these entities to finish all these testing scenarios. Minor defects were identified during the testing, and MRO is working with NERC to fix these defects. MRO would like to thank Evergy, Oklahoma Municipal Power Authority, and Xcel Energy for their participation in Align testing.

The Align Project Team is working on training materials, videos, and start-stop-continue guides in preparation for Release 1 training. Training dates will be provided once an official go-live date for Release 1 has been identified. Training will be provided to MRO and Texas RE regional staff and registered entities first as they will be piloting the Align system. Please remember each Align user will be required to setup an ERO portal account prior to being able to utilize Align. You can register for an ERO portal account here: https://www.nerc.com/Pages/AccountLoginRegister.aspx, if you do not already have one.

On June 22, 2020, FERC issued a delegated letter order approving NERC’s financing request for the development of the ERO Secure Evidence Locker (SEL), which will be implemented in conjunction with Align Release 1 in 2021. The ERO SEL will be used for the collection and analysis of evidence provided by registered entities in support of the Compliance Monitoring and Enforcement Program. The ERO SEL will greatly improve the security of how the ERO Enterprise collects, manages, and disposes of sensitive information. The SEL is currently in the design phase.

Any entity that plans to build its own Secure Evidence Locker should read the design requirements posted on NERC’s website here: https://www.nerc.com/ResourceCenter/Align%20Documents/1-Align-Registered%20Entity%20SEL%20Functional%20Requirements%20Updated%20April%202020.pdf.

If your entity is planning to utilize its own Secure Evidence Locker, please e-mail the MRO Align Change Agents, Marissa Falco and Desirée Sawyer. Questions on Align or the SEL should be submitted to askalign@nerc.net, or reach out to your MRO Align Change Agents. You may also find helpful information on NERC’s Frequently Asked Questions page on the Align Project Page.

-Marissa Falco, Risk Assessment and Mitigation Administrator
Securing Sensitive Documentation

In an industry where security, both physical and electronic, are paramount to the reliability of the Bulk Electric System (BES), it is very important that everyone is aware confidential information may be forced to become public. This means that entities need to ensure that their information is secured properly. The Evidence Request Tool (ERT) has a disclaimer that states “Please be aware of the Labeling Guidance for ERO Enterprise Documents and ensure to follow the proposed marking of documentation appropriately.” The contents of this article will help explain what this message means and why it’s so important.

In order to properly protect your confidential information from potential Freedom of Information Act (FOIA) exposure, it’s important that documentation is properly labeled. A summary of the guidance from FERC on how to properly label documentation is as follows:

“Documents containing Critical Energy/Electric Infrastructure Information (CEII)...should include in a top center header of each page of the document the following text: CUI//CEII.”

“Documents containing information that [FERC] recognizes as privileged, and documents containing information within the scope of protective orders and agreements in Commission proceedings, should include in a top center header of each page of the document the following text: CUI//PRIV.”

“Documents containing multiple information types, should reference each information type in a top center header of each page of the document in the following format: CUI//[Information Type]/[Additional Information Type], e.g., CUI//CEII/PRIV.”

The ERO Enterprise already has a few measures in place to ensure this labeling is being enforced. CIP-011-2 – Cyber Security – Information Protection is a NERC standard that requires “Method(s) to identify information that meets the definition of BES Cyber System Information.” One such method is proper labeling of documents based on the previously listed guidance.

The protection of sensitive information is paramount in a world where sensitive information can be requested by the general public if circumstances line up. Having this sensitive information available to anyone is detrimental to the security and reliability of the BES. By ensuring your documentation is properly labeled, whether adhering to the NERC standards or following through on the ERT disclaimer, you are doing your part to ensure continued stability throughout the BES.

-Elliot Weishaar, CIP Compliance Engineer

References:


Compliance Insight Regarding Reliability Standard PRC-004-5

MRO considers proper analysis of interrupting device operations to be fundamentally significant to the reliability of the Bulk Electric System (BES). Our approach for reviewing compliance with NERC Reliability Standard PRC-004-5 (PRC-004-5) analyzes the entity’s methodology of discovering, assessing, and mitigating issues related to misoperations. This article will discuss PRC-004-5 requirements and provide a little insight to MRO’s compliance approach to PRC-004-5(i) oversight. It will also highlight the importance of internal controls for compliance, but also for reliability of the BES.

There is a distinct difference between adherence to the PRC-004-5, and the purpose of NERC’s Misoperation Information Data Analysis System (MIDAS) reporting. The purpose of PRC-004-5 is to identify and correct the causes of misoperations for BES elements, while the purpose of MIDAS reporting is to monitor, analyze, and track trends in Protection System Misoperations to improve BES reliability. PRC-004-5 does not have periodic reporting requirements; instead it places a timeframe limit of 120 days for the identification of the cause of any operation. MIDAS on the other hand, requests entities to report data on a quarterly basis, within 60 days of the end of each quarter to the MIDAS NERC Portal. PRC-004-5 and the MIDAS reporting process are applicable to Transmission Owners, Generator Owners, and Distribution Providers.

In our experience, we have found that entities tend to write misoperation programs that adhere to MIDAS requests rather than follow the requirements of PRC-004-5. MIDAS captures R1 initial analysis, R4 continued analysis of an unknown cause, in addition to Corrective Action Plan (CAP) mitigation under R5 and R6. While creating a combined program document in order to speak to both PRC-004-5 and the MIDAS submittal requirements is understandable and acceptable, the result often unintentionally does not cover the details of R2 and R3 regarding the different notifications required to comply with the standard. The purpose of MIDAS and its more frequent reporting obligations should not overcast the standard’s purpose and compliance requirements.

PRC-004-5 R1 states that an entity needs to identify the component that caused device operation whether it is a justified operation or a misoperation. This indicates that the evidence of analysis should not be limited only to the suspected misoperations. MRO’s audit approach requests a list of all device operations for a certain time period. The audit team will sample these operations and will review an entity’s analysis evidence of both legitimate/justified device operations and misoperations. MRO’s review goes through the entity’s submitted documents to verify that an analysis of the different device operations was conducted.

PRC-004-5 R2 defines the reporting responsibilities relative to joint ownership. It is expected that all joint owners communicate and share information for analysis, however there have been occasions when MRO has experienced when an entity is unclear on who is responsible for the official notification and when notification is required. The owner of the device that operated (the device that cleared the abnormal condition) is the entity responsible for providing the notifications required by PRC-004-5 R2.

The owner of the operating device is responsible, per R2, to provide notification within the established time frame (120 days) and, per R2.1, to have a preliminary cause determination that either the operation was a misoperation, but was not caused by their own protection system component, or if they were unable to determine if the device operation was a misoperation. It is important to mention that the “notifications” required
include those between Generator Owners (GOs) and Transmission Owners (TOs) of the same company, if analysis is completed by separate groups. Notifications regarding backup protection (covered under R2.2.) follow similar responsibility as the entity providing the backup protection (a correct operation) is required to notify the other protection system owner(s). These notifications to co-owners follow the intent of the standard by helping to ensure analysis for BES interrupting devices that did not operate. More detailed information and examples can be found in the PRC-004-5(i) Standard Application Guide Version 1.1 published on March 22, 2017.

PRC-004-5 R5 states that an entity is required to complete an evaluation of the CAP’s applicability to the entity’s other Protection Systems, including other locations. MRO’s different teams have encountered situations where a CAP was developed, but an evaluation for the CAP’s applicability to other Protection Systems and other locations was not completed. During the process of reviewing sampled CAPs, the MRO audit team will seek verification that an entity completed an evaluation of applicability to other locations regardless of the misoperation cause. One of the most common reasons for a misoperation provided by entities is “human error,” which includes, but is not limited to incorrect settings, logic errors, as-left personal errors, and design errors. MRO’s stance is that even issues arising from human error should have an evaluation of applicability completed. If the entity doesn’t believe that the cause of the misoperation is applicable to multiple locations on its system, the entity would need to show evidence describing how and why that conclusion was reached.

For MRO to reach reasonable assurance, and as part of good internal controls, the entity needs to ensure proper documentation is retained to demonstrate compliance...

For MRO to reach reasonable assurance, and as part of good internal controls, the entity needs to ensure proper documentation is retained to demonstrate compliance; in other words, “show your work.” MRO will review an entity’s effectiveness of design and implementation that may identify industry best practices, recommendations and areas of concern.

Due to the inherent risk of PRC-004-5, internal controls are a key focus of MRO’s compliance activities. It is also important in the sense that internal controls can help inform future monitoring and Compliance Oversight Plans. One final note on PRC-004-5 and internal controls - there is strong agreement across the ERO Enterprise that applying effective internal controls can significantly reduce misoperations.

Protection System misoperations continue to be a leading cause in the initiation of BES events. Continued review of best practices and methods for protection system misoperation identification and correction can only help to improve the misoperation rate.

If there are any questions, please contact heros@mro.net.

-Summer Stephens, Compliance Auditor, and Rafik Halim
Industry Tips and Lessons Learned

For the most current information regarding NERC standards and compliance, see the NERC Standards, Compliance, and Enforcement Bulletin. Bulletins from the past year are maintained on the Standards site and the Compliance and Enforcement site. To access them, navigate to the Standards page or Compliance and Enforcement page, scroll to the bottom where the five most recent bulletins are displayed, and select the “Standards, Compliance, and Enforcement Bulletin Archive” link.

Since MRO’s last publication, the following lessons learned have been posted on NERC’s website on the Lessons Learned page:

- **Lockout Relay Component Failure Causes Misoperation and Reportable Event**
- **Verification of AC Quantities during Protection System Design and Commissioning**
- **Mixing Relay Technologies in DCB Schemes**
- **Preventing Energy Emergency Alerts**
- **Unanticipated Wind Generation Cutoffs during a Cold Weather Event**

A successful Lesson Learned document clearly identifies the lesson, contains sufficient information to understand the issues, visibly identifies the difference between the actual outcome and the desired outcome and includes an accurate sequence of events, when it provides clarity.

Webinar Resources Posted

- NERC posted the slide presentation and recording for the Project 2015-09 – Establish and Communicate System Operating Limits webinar.
- NERC posted the slide presentation and recording for the Project 2016-02 – Modifications to CIP Standards SuperESP webinar.
- MRO posted the presentations and recording for the recent webinar on Internal Controls: Use of Templates, hosted by the CMEP Advisory Council.
- MRO’s Security Advisory Council (SAC) has hosted several webinars in 2020, and recordings of those webinars are available on the SAC Outreach Page of MRO’s website.
- MRO’s Reliability Advisory Council (RAC) has hosted two webinars so far this year, and recordings of those webinars are available in MRO’s video library on the RAC Outreach Page.
Compliance Monitoring and Enforcement Program Update

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

Compliance Oversight Plans (COPs)

MRO participated in collaboration with the North American Electric Reliability Corporation (NERC) and the other Regional Entities in a joint effort to have common inputs and reports for performing COPs. MRO’s process for performing COP’s involves input from the RAPA, RAM, Registration, Compliance, and Enforcement Departments. The resulting COP from this process documents MRO’s holistic assessment of the registered entities’ inherent risk and the performance considerations assessing the entities’ management of risk. The resulting COP guides MRO’s monitoring activities. The MRO Compliance Department received approval from NERC on MRO’s implementation of the aligned COP process. MRO has established a schedule for developing COPs per the new Electric Reliability Organization (ERO) COP process for 2020. The first COP under this revised process was issued in May and the second COP was issued in June.

2020 Compliance Audit Status

MRO staff completed 8 of 16 scheduled compliance audits for 2020. Given the impacts of COVID-19 on registered entities, two audits that were originally scheduled for 2020 are being rescheduled to be performed in 2021. Additionally, one audit was cancelled secondary to the results of the entity’s Inherent Risk Assessment. MRO will provide resources to participate in 8 coordinated oversight audits led by other Regional Entities in 2020. Please visit MRO’s website to view MRO’s 2020 audit schedule.

2020 Self-Certifications

MRO revised the Self-Certification scoping process. The risks identified in MRO’s Regional Risk Assessment and the ERO Enterprise CMEP Implementation Plan are now the two primary considerations. The advantage of using Self-Certifications is that it allows MRO to address continent-wide risks and region-wide risks across MRO’s footprint through a single process at a faster interval than audits would allow. MRO has been receiving responses to the Q2 2020 Self-Certification for Cyber Security-Information Protection (CIP-011-2) and Transmission Operations (TOP-001-4), that because of the extended due date, are now due by September 30, 2020. MRO issued Q4 Self-Certifications for Cyber Security-Personnel & Training (CIP-004-6) and Transmission System Planning Performance (TPL-001-4) on July 1, 2020. 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 answer questions submitted to Heros@mro.net. This tool is widely used by MRO registered entities and serves as a great mechanism for compliance related questions. MRO has received a total of 332 questions through this email address since it was implemented in November of 2016. Over the last quarter, we have received 31 questions with an average response time from MRO to the entity of 9 days.

Expanded COVID-19 Reporting Guidance

Previously, MRO utilized the HEROS email as a communication tool for any intentional non-compliance performed in response to the coronavirus outbreak, including periodic requirements; however, that process changed after
NERC provided expanded guidance for the reporting of potential noncompliance related to COVID-19. Regulatory discretion has been expanded to include any potential noncompliance from March 1, 2020, through the end of the year, where COVID-19 contributes materially to the root cause. The ERO Enterprise recognizes the fluidity of this emergency and will reassess the timeline if needed. MRO registered entities should report potential noncompliance due to COVID-19 through MRO’s FTP3 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 is not necessary for these issues. For more guidance on this process please refer to the information provided in MRO’s Hot Topic for this, in addition to the update provided on August 13.

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

As of July 30, 2020, there are 31 MRO entities participating in the Self-Logging program. As reported by NERC, in addition to MRO’s 31 participants, the number of participants for the other ERO Regional Entities are as follows: ReliabilityFirst:16; Northeast Power Coordinating Council, Inc.:13; SERC Reliability Corporation: 11; Texas RE: 10; and Western Electricity Coordinating Council: 8. MRO, as compared to the rest of the ERO, has the greatest number of participants and accounts for 35 percent of all ERO Self-logging participants (see Fig. 1) for all percentages. Self-Logged instances submitted by these participants are monitored separately to aid in processing timeliness as the program is designed to quickly resolve minimal risk issues that were self-identified by entities. These issues are presumed minimal risk and to be processed as compliance exceptions. The RAM department is continually evaluating its process and outreach to improve processing efficiencies and validation of minimal risk non-compliance. This past quarter, for example, RAM has implemented a new intake process to assist in the efficient processing of newly identified non-compliances.

Fig. 2 on page 18 trends self-logged instances of noncompliance by their submittal dates, and shows that other than two self-logs in Q4 of 2017, the oldest self-log to be processed is from 2019. These two 2017 self-logs are part of a larger group of noncompliances for a particular entity which required lengthy extent of condition reviews. Please note submittal dates are not when the potential noncompliance occurred 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 current MRO region.

Compliance Severity Index (Figure 3)

MRO staff uses the Compliance Severity Index (CSI), shown in Fig. 3, to evaluate progress towards 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.” While not all noncompliances from 2016-present have been processed, MRO has seen a notable decrease in the risk of noncompliances over the past ten years, with one particular compliance engagement contributing to an uptick in 2016.
Highest Risk Noncompliances (Figure 4)

Fig. 4 provides the 15 highest risk requirements from January 1, 2016, to July 31, 2020, that have a history of noncompliance, based on the CSI. MRO has seen a steady trend towards more CIP requirements dominating this metric, in addition to Facility Ratings (FAC-008) and Protection System Maintenance (PRC-005). PRC-005 has steadily been decreasing over time, since previously being the highest risk noncompliance in the MRO region.

Risk Determinations for Instances of Noncompliance (Figure 5)

Ninety-one percent of all instances of noncompliance from January 1, 2016, to July 31, 2020, 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 they become more impactful to the reliability and security of the BES. This is emblematic of HEROs.
Noncompliance Trends and Statistics

Breakdown of CIP vs. Non-CIP Possible Noncompliances (Figure 6)

The noncompliance statistics and trends in Fig. 6 are by year discovered and reported to NERC from January 1, 2011, to July 31, 2020. The increase in noncompliance in 2018 and 2019, is due to an increase in registered entities related to the SPP RE transition. Also, there was a substantial increase in self-logging registered entities which could, in turn, lead to an increase in reported issues of noncompliance. Self-logging allows entities a more convenient and streamlined method of reporting minimal risk items. Typically, MRO sees more self-identified minimal risk issues being reported by self-logging entities. Therefore, as the number of MRO self-logging entities increases, the number of noncompliances may increase. The CSI shows that although the number of noncompliances have gone up, MRO self-logging entities are self-identifying issues early that are of minimal risk, and aligned with HERO principles.

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 for both metrics, reflected in Fig. 7 and Fig. 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.

Fig. 7 on page 21 reflects instances of noncompliance that MRO processed from January 1, 2011, to July 31, 2020.

Fig. 8 on page 21 shows the percentage of time that registered entities have accepted responsibility for noncompliance submitted to NERC or another applicable Regulatory Authority from January 1, 2011, through July 31, 2020.

In Fig. 9 on page 21, the numbers reflect all noncompliances in the MRO region that were reported to NERC from January 1, 2011 through July 31, 2020.
Fig. 7: Self-Identified Noncompliance

Fig. 8: Registered Entity Acceptance of Responsibility
(January 1, 2011 - July 31, 2020)

Fig. 9: Discovery Method

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance Audit</td>
<td>62</td>
<td>71</td>
<td>71</td>
<td>27</td>
<td>12</td>
<td>25</td>
<td>23</td>
<td>33</td>
<td>46</td>
<td>17</td>
<td>387</td>
<td>90</td>
<td>297</td>
</tr>
<tr>
<td>Compliance Investigation</td>
<td>0</td>
<td>10</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>10</td>
<td>1</td>
<td>9</td>
</tr>
<tr>
<td>Data Submittal</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Self- Certification</td>
<td>44</td>
<td>9</td>
<td>11</td>
<td>4</td>
<td>3</td>
<td>11</td>
<td>2</td>
<td>23</td>
<td>7</td>
<td>0</td>
<td>114</td>
<td>32</td>
<td>82</td>
</tr>
<tr>
<td>Self-Log</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>6</td>
<td>50</td>
<td>99</td>
<td>132</td>
<td>77</td>
<td>365</td>
<td>6</td>
<td>359</td>
</tr>
<tr>
<td>Self-Report</td>
<td>70</td>
<td>50</td>
<td>67</td>
<td>28</td>
<td>47</td>
<td>90</td>
<td>74</td>
<td>73</td>
<td>83</td>
<td>51</td>
<td>633</td>
<td>86</td>
<td>547</td>
</tr>
<tr>
<td>Spot Check</td>
<td>11</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>14</td>
<td>4</td>
<td>14</td>
<td>4</td>
<td>10</td>
</tr>
<tr>
<td>Totals</td>
<td>187</td>
<td>141</td>
<td>149</td>
<td>59</td>
<td>63</td>
<td>132</td>
<td>151</td>
<td>228</td>
<td>268</td>
<td>145</td>
<td>1523</td>
<td>219</td>
<td>1304</td>
</tr>
</tbody>
</table>
COMPLIANCE MONITORING AND ENFORCEMENT PROGRAM

Noncompliance Processing (Figures 10 and 11)

MRO staff analyzes trends in the status of noncompliance processing using the composition of 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. Fig. 10 and Fig. 11 include noncompliances for entities that were registered in the MRO region during the specified time periods.

Status of Alleged and Confirmed Instances of Non-Compliance (Figure 12)

Fig. 12 includes the number of noncompliances for entities that were registered in the MRO region from June 18, 2007, through July 31, 2020.

<table>
<thead>
<tr>
<th>Fig. 12: Status of Possible Noncompliance</th>
<th>Total</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Number of Findings</td>
<td>1843</td>
<td>100%</td>
</tr>
<tr>
<td>Number of Dismissals</td>
<td>317</td>
<td>17%</td>
</tr>
<tr>
<td>Number of Findings Processed</td>
<td>1234</td>
<td>67%</td>
</tr>
<tr>
<td>Number of Findings Awaiting Filing or Posting</td>
<td>15</td>
<td>1%</td>
</tr>
<tr>
<td>Number of Findings Outstanding</td>
<td>277</td>
<td>15%</td>
</tr>
</tbody>
</table>

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
It is widely understood that owners, users, and operators of the bulk power system are registered in the NERC Compliance Registry (NCR) and are responsible for compliance with NERC Reliability Standards. While there are a few questions related to larger entities, more questions tend to arise from smaller entities or shared ownership regarding registration. The NERC Rules of Procedure (ROP) identify three options for registration of these entities, (1) Functional Registration, (2) Joint Registration Organization (JRO), and (3) Coordinated Functional Registration (CFR).

Prior to registration of the owners of generation and transmission assets, it is necessary to determine if those assets meet the criteria of being a Bulk Electric System (BES) asset. In general, BES assets are, “… all Transmission Elements operated at 100 kV or higher and Real Power and Reactive Power resources connected at 100 kV or higher. This does not include facilities used in the local distribution of electric energy.” The full definition of BES is available in NERC ROP, Section I of Appendix 5B Statement of Registry Criteria. The application of the definition of BES is purely focused on the physical attributes of the facility and does not take ownership into consideration. Ownership is taken into consideration in the registration process.

The majority of BES facilities are owned by a single entity, simplifying the registration in the NCR as an owner. The NCR is the registration of the entities performing functions; registration in the NCR is not an inventory of assets. Once an entity is registered as an owner, the entity is not required to register every time a BES asset is added to their inventory. However, it is common for independent power producers to request registration at the facility level. Therefore, MRO requests Generator Owners and Transmission Owners to provide updates to their Facility Verification forms as they add or remove assets from their inventory.

Although single ownership of facilities is the most common, shared ownership of both generating and transmission facilities is not unusual. Shared ownership does not change the physical characteristics of the facility. For example, a dispersed generating facility owned by three entities, each owning 30 MVA of generation, are recognized as owners of a 90 MVA facility. It is up to the owners of the facility to determine if one entity will register as the owner in the NCR or if all owners will register independently. While the registration of only one entity as the owner may provide efficiencies for both the ERO Enterprise and the owners, there may be business reasons to maintain independent registrations.
While JROs and CFRs are available for entities that own an entire facility that desire to delegate their responsibilities, these two agreements are also good options for those entities sharing ownership of facilities as well. Registration of JROs and CFRs memorializes operating agreements amongst two or more entities through the NERC Registration process.

A JRO is the clearest and simplest delegation of responsibility between the JRO and CFR options. A JRO is an agreement between two or more entities, in which one entity accepts full responsibility for one or more functions. For example, the ownership of a BES generating facility with six combustion turbines rated at 50 MVA, may be split 5/1. The owner of the five turbines may also be performing compliance-related tasks for the additional turbine and find it more efficient to accept responsibility for compliance with the NERC Standards and enter into a JRO, accepting responsibility as the Generator Owner.

The CFR option on the other hand, delegates only a portion of the requirements. Using the same generator facility example above, the owner of the one unit may perform Protection System maintenance on its own generator, and delegate the remaining tasks associated with compliance to the majority share owner of the facility. In addition to the agreement between the two entities, the entity responsible for submitting the CFR is required to maintain a CFR matrix through the ERO Portal that assigns responsibility of each requirement related to the functions.

The ERO Enterprise is responsible for ensuring all generation and transmission facilities are classified properly as BES assets, or not. Neither ownership, nor the point at which ownership transfers, are taken into consideration in determining BES assets. Ownership is given consideration only during the registration process. The ERO Enterprise ensures there are no gaps in compliance monitoring by ensuring entities providing the associated functions have been identified and are appropriately registered.

Questions related registration should be sent to registration@mro.net.

Certification Reviews

All Balancing Authorities (BAs), Reliability Coordinators (RCs), and Transmission Operators (TOPs) registered in the NERC Compliance Registry are certified to perform their respective functions. The certification process 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 applicable NERC Reliability Standards. Certification is not a periodic activity. Once certified, entities are not subject to any additional certification process, as long as no material changes to their scope of operations have occurred.

Any BA, RC, or TOP that experiences a material change to their operations are considered candidates for a Certification Review. Reviews are a condensed version of the certification process, focusing solely on the change affecting the entity’s real-time operations. The most common triggers for a Certification Review are the complete replacement of an existing SCADA/EMS, relocation of a control center, or a change of footprint. For a complete list of changes subject to review, see section IV of the NERC Rules of Procedure, Appendix 5A – Organization Registration and Certification Manual.

Just as with Certifications, Certification Reviews are not compliance monitoring activities. While it is true the basis for a large component of the certification review engagement is the NERC Reliability Standards, both types of engagements are forward looking. The focus is an assessment to determine if the necessary tools, trained staff, processes, procedures, and cyber and physical controls are in place. Areas of concern identified during the engagement provides the opportunity for the registered entity to make corrections with no compliance implications. As part of the engagement, registered entities may receive non-binding recommendations for consideration. Registered entities have discovered that Certification Reviews provide one more level of assurance. The Certification Review Team is comprised of experts who have worked with other registered
entities that have experienced similar changes to their operations and are familiar with any obstacles or issues the entity may experience as a result of the changes in operations.

Any entity registered within MRO’s region, planning on a change, or having questions related to a potential change, should contact MRO at certification@mro.net.

Standards Update

The Federal Energy Regulatory Commission (FERC) Order approving Reliability Standard PRC-024-3: Frequency and Voltage Protection Settings for Generating Resources, has the greatest impact on the owners of inverter based resources (e.g., solar photovoltaic (PV) and wind power resources). The revised standard contains a series of edits and clarifications intended to ensure inverter-based resources, in addition to the currently required generators, respond to grid disturbances in a manner that contributes to the reliable operation of the bulk power system.

The standard was revised to address recommendations of the NERC Inverter-Based Resource Performance Task Force. These recommendations were developed in response to the findings and recommendations of the NERC and WECC analysis of the Blue Cut Fire and Canyon 2 Fire disturbances in southern California. The effective date for PRC-024-3 is October 1, 2022.

FERC’s letter approving BAL-003-2 Frequency Response and Frequency Bias Setting completes the Phase I portion of a two-phase project. Phase I of the project revised the BAL-003-1.1 standard and process documents to address: (1) the inconsistencies in calculation of Interconnection Frequency Response Obligations (IFRO) due to Interconnection Frequency Response performance changes of Point C and/or Value B; (2) the Eastern Interconnection Resource Contingency Protection Criteria; (3) the frequency of nadir point limitations (currently limited to t0 to t+12); (4) clarification of language in Attachment A, (i.e., related to Frequency Response Reserve Sharing Groups (FRSG) and the timeline for Frequency Response and Frequency Bias Setting activities); and (5) enhancements to the BAL-003-1 FRS Forms that include the ability to collect and submit FRSG performance data. Additionally, the supporting procedural and process steps have been removed from Attachment A and captured in the Procedure for ERO Support of Frequency Response and Frequency Bias Setting Standard.

Phase II of the BAL-003 project will address making the IFRO calculations and associated allocations: 1) more reflective of current conditions; 2) consider all characteristics affecting Frequency Response (e.g., load response, mix and type of generation); 3) include all applicable entities; and 4) be as equitable as possible. Phase II will also address Frequency Response Measure (FRM): 1) ensure that over-performance by one entity does not negatively impact the evaluation of performance by another; 2) measure types/periods of response in addition to secondary Frequency Response, particularly primary Frequency Response; 3) include all applicable entities; and 4) make allocations as equitable as possible. The effective date of BAL-003-2 is December 1, 2020.

For details regarding Reliability Standards within your governing jurisdiction:
Manitoba: Reliability Standards Regulation
Saskatchewan: SERA Adopted Standards
United States: NERC One-Stop-Shop

-Russ Mountjoy, Manager of Registration, Certification and Standards
Substation Equipment Failure

The safe and reliable operation of the bulk power system (BPS) depends on the facilities and control devices within the BPS being in normal operating condition. Equipment failure can have significant impact on system reliability depending on the failure type and the severity of the failure.

Equipment and material failure has been a major contributor to system events with extended outage time.

Equipment failure impacts vary from minimal to catastrophic. A blown power fuse on a microprocessor relay might only affect the operability of that particular relay, while an open circuited current transformer can have catastrophic affects that result in equipment damage, extended outage time, and potential loss of life. Fortunately, many of these types of equipment failures have known and recognizable warning signs that can be used to lessen, or even prevent, the failure through appropriate and timely maintenance.

Failure modes are the obvious effects of equipment failure where a piece of equipment fails to accomplish its intended function or operates in an undesired fashion. Equipment failure can have varying levels of complexity and severity. Understanding the complexity of a particular failure mode and what early signs of this failure look like, can be a valuable tool in mitigating it. Failure mechanisms are the path that lead to an imminent failure mode, and can provide indications of an imminent failure. Armed with this valuable data along with appropriate situational awareness, planning and development of preventative maintenance schedules for various types of equipment can be accomplished more effectively,
To this end, the Failure Modes and Mechanisms Task Force (FMMTF) was approved by the NERC Event Analysis Subcommittee (EAS) in December 2019. The purpose of the FMMTF is to analyze common Bulk Electric System (BES) substation equipment failures and determine their failure modes and mechanisms. The FMMTF is made up of 14 participants consisting of NERC staff and stakeholders. Meetings are held monthly where Failure Modes and Mechanisms (FMM) diagrams are discussed and developed. The diagrams describe failure modes common to a specific piece of equipment and the different, known failure mechanisms that lead to those failure modes. Below is what a typical FMM diagram looks like. The Capacitor Bank diagram is shown here:

FMM diagrams currently being developed are:

- Oil-Filled Power Transformer
- Instrument Transformers (PTs & CTs)
  - Wire Wound Electromagnetic Potential Transformer
  - Coupling Capacitor Voltage Transformer
  - Optical Voltage Transformer
  - Wire Wound Electromagnetic Current Transformer
  - Optical Current Transformer
- Circuit Breakers
  - SF6 Breaker
  - Air Blast Breaker
  - Oil Breaker
NERC Reliability Standard PRC-012-2 will become effective January 1, 2021, and the Planning Coordinators (PC) and Reliability Coordinators (RC) in the MRO region are already taking steps towards this transition. There are four PCs in the region: Manitoba Hydro (MH), Midcontinent Independent System Operator (MISO), Saskatchewan Power Corporation (SPC), and Southwest Power Pool (SPP). The three RCs in the region—MISO, SPC, and SPP—are also PCs. These PCs and RCs have a wide area view of the Bulk Electric System (BES) in the region, and are responsible for long term planning, resource adequacy, real-time congestion management, and also have the authority to issue emergency operating procedures.

A Remedial Action Scheme (RAS) as defined in the NERC Glossary, is a scheme designed to detect predetermined system conditions and automatically take corrective actions that may include, but are not limited to, adjusting or tripping generation (MW and MVAR), tripping load, or reconfiguring a System. RASs accomplish objectives such as maintaining BES stability, maintaining acceptable BES voltages and thermal limits, and limiting the impact of cascading or extreme events. Entities normally install these schemes as a temporary fix or operator convenience until the transmission system is upgraded. MRO’s Special Protection System Working Group currently reviews all new, modified, or retiring RASs in the MRO region (See June SPSWG Article). MRO has been working with its PCs and RCs to transition this review per PRC-012-2.

Remedial Action Schemes

Transition of Responsibility in PRC-012-2

NERC Reliability Standard PRC-012-2 will become effective January 1, 2021, and the Planning Coordinators (PC) and Reliability Coordinators (RC) in the MRO region are already taking steps towards this transition. There are four PCs in the region: Manitoba Hydro (MH), Midcontinent Independent System Operator (MISO), Saskatchewan Power Corporation (SPC), and Southwest Power Pool (SPP). The three RCs in the region—MISO, SPC, and SPP—are also PCs. These PCs and RCs have a wide area view of the Bulk Electric System (BES) in the region, and are responsible for long term planning, resource adequacy, real-time congestion management, and also have the authority to issue emergency operating procedures.

A Remedial Action Scheme (RAS) as defined in the NERC Glossary, is a scheme designed to detect predetermined system conditions and automatically take corrective actions that may include, but are not limited to, adjusting or tripping generation (MW and MVAR), tripping load, or reconfiguring a System. RASs accomplish objectives such as maintaining BES stability, maintaining acceptable BES voltages and thermal limits, and limiting the impact of cascading or extreme events. Entities normally install these schemes as a temporary fix or operator convenience until the transmission system is upgraded. MRO’s Special Protection System Working Group currently reviews all new, modified, or retiring RASs in the MRO region (See June SPSWG Article). MRO has been working with its PCs and RCs to transition this review per PRC-012-2.
Each RAS is unique and its actions can have a significant impact on the reliability and integrity of the BES; therefore, a review of a proposed new RAS or an existing RAS proposed for functional modification or retirement must be completed prior to implementation. This review involves data such as transmission maps, one-line drawings, substation, and schematic drawings that identify the physical and electrical location of the RAS and related facilities. Other important items of focus are contingencies and system conditions that the RAS is intended to remedy, and action to be taken by the RAS in response to disturbance conditions. When redundancy of the RAS is required, the entity will also submit logic diagrams and system protection and communication diagrams to verify that a single point of failure cannot compromise the RAS.

Below is a process flow diagram from the PRC-012-2 standard. This diagram illustrates the many different paths a RAS review can take depending on if it’s a new scheme, a five-year review, RAS operation, or retirement.

- Bryan Clark, PE, MRO Director of RAPA
MRO Generator Cold Weather Preparation Pilot Program

MRO is pleased to announce the formation of the Generator Cold Weather Preparation (GCWP) program pilot, implemented by the MRO Reliability Assessment and Performance Analysis (RAPA) Department. MRO will perform assessments of select generating facilities and their preparation for cold weather events in an effort to minimize cold weather related generation outages.

The MRO region is accustomed to cold weather as its footprint extends to the provinces of Manitoba and Saskatchewan. At the same time, MRO reaches south to the more temperate gulf states of Louisiana and Texas, which do not experience the routine extreme cold temperatures of the northern part of the region. This diversity of climates results in vast differences in the construction characteristics of generation systems throughout the region. As a result, not all facilities are designed or prepared for the weather anomalies such as the Southwest Cold Weather Event of February 2011; the Polar Vortex of January 2014; and most recently, the South Central United States Cold Weather Bulk Electric System Event of January 2018.

The GCWP will focus its efforts on new generation facilities and existing facilities generating 500 MW of load or greater. Selected facilities will receive a survey questionnaire related to their cold weather preparations, and a potential site visit by MRO staff if necessary. MRO staff will review winterization plans, processes and procedures, and if necessary perform a walk-down of the facility, and will provide notable observations to the facility owner(s). Upon completion of any visits, the registered entity will receive a summary report of its cold weather preparation efforts and any non-binding recommendations the team may have for improvement. As the program is implemented, MRO will share any best practices, offering other generator owners the opportunity to enhance their processes related to cold weather preparation.
MRO is collaborating with staff from other Regional Entities in the development of the GCWP in 2020, with site visits expected to commence in 2021. MRO staff recently joined ReliabilityFirst staff on an on-site visit of a new generation facility. Texas Reliability Entity (TexasRE) joined forces with Electric Reliability Council of Texas (ERCOT) in developing a generator winterization program which has matured over the past few years. The two organizations will be co-hosting the ERCOT and Texas RE Generator Winter Weatherization Workshop on September 3, 2020, which is open to all interested stakeholders. This collaboration of efforts with other Regional Entities is providing greater efficiencies and effectiveness across the ERO Enterprise as we address generation preparation for cold weather.

-Russ Mountjoy, Manager of Registration, Certification and Standards

Conference Details

Midwest Reliability Organization’s Reliability Advisory Council is pleased to announce it will host the 2020 Reliability Conference via WebEx. This one-day conference will focus on several current planning and operating topics that are important in the MRO region.

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

Planned Agenda Topics

- NERC Electric Gas Working Group
- Inverter Based Resource Performance Task Force
- Storage Technology
- Waupaca Area Storage Project
- Distributed Energy Resources in System Operation

The agenda is available here. To register to attend this virtual conference, click here. Registration closes on August 24, 2020.
Cyber Asset Focused Risk Assessments

One of the most significant challenges in building and refining any organization’s cyber security program is trying to prioritize resources. With limited time and financial resources, prioritizing those resources to reduce the greatest amount of risk in an ongoing risk management activity.

A robust cyber security program has a risk management program component that is intended to do just that - assist in the prioritization of the organization’s resources. A risk management program documents how an organization conducts the risk assessments that are used to identify and quantify risks to the organization. A well-designed program also assists the organization in identifying and prioritizing mitigation activates to reduce the risks identified in the risk assessment.

There are a variety of common risk assessment methodologies at use in the Electric Sector. One prevailing framework is documented in NIST 800-30 Rev 1 (link). Another common framework is the Center for Internet Security Top 20 Critical Cyber Security Controls (link). Additionally, there are several vendors or trade organizations that have their own risk assessment frameworks or tools.

The challenge with most risk assessment methodologies is they are focused at the organization level, meaning they ask questions that are intended to evaluate the organization as a whole, not necessarily individual cyber assets or cyber systems. Risk assessments with an organizational focus are an excellent starting point for organizations that are new to risk management. These types of high level assessments are
great at providing an overview of an organization’s risk profile, as measured by the assessment, as an input to leadership or a board of directors. However, they have limitations, especially for large organizations.

Risk assessments that provide an organization-level view make it harder to distinguish between business units within an organization. For example, if the assessment asks if you are conducting regular data back-ups and your IT (Information Technology) team does (High), but your OT (Operations Technology) team does not (Low), how do you answer? The result tends to be a mixing of answers. In this example, we take the “High” response from IT and the “Low” response from OT, and we say that as an organization, we have a Medium score. While this does work, the process runs the risk of masking significant risks that may exist by inadvertently hiding the results.

As you work to continue to refine your organization’s risk management program, you want to look for ways to continue to improve upon your ability to more clearly and accurately identify risk. An alternative method is to take your risk assessment to the cyber asset or cyber system level.

In this asset focused methodology, you would take cyber assets or cyber systems and perform a risk assessment against them, grouping like assets that share attributes to assist in streamlining the process. For example, you can group most of the desktop computers at a location and evaluate them as one asset. However, it may be advisable to break out desktop computers used by IT or OT administrators, as they may represent a higher degree of inherent risk.

For this type of risk assessment to be successful, it is essential that the organization works toward implementing a cyber-asset management program that allows the identification of all cyber assets and cyber systems owned by the organization. I cannot understate the importance of the identification of assets in a robust cyber security program. You cannot adequately protect an asset if you do not know it exists.

In an asset-focused risk assessment, the goal is to prioritize your assets, identify and prioritize threats to the asset, and identify controls to mitigate the threats. Keep in mind that each asset should have multiple threats, which can be human-made or naturally occurring, and that each threat may apply to multiple assets. In turn, each control you identify can mitigate multiple threats across multiple assets. Ideally, this results in a “many to many to many” relationship between assets, threats, and controls. This relationship allows you to see the impact of threats and controls across your environment.

There are various means available to quantify this process. You can score each asset based upon the CIA (Confidentiality, Integrity, and Availability) triad to aid in identifying asset criticality. Threats can be scored using probability and impact. These scores can even vary from asset to asset, which helps in determining the greatest threats to each asset. Controls can even be scored to help you determine how much risk each control mitigates. You can also identify a control even if you cannot implement it. This method allows you to show that there are other ways to mitigate the risks that you may or may not be able to achieve now or in the future, and will provide more accurate and nuanced scoring. There are various resources available on scoring assets-in an asset focused risk assessment that are beyond the scope of this article.
The goal of the process is to assist you in prioritizing your assets using a consistent metric across your organization. By identifying the threats to those assets, you can begin to identify areas of risk. Controls are, in turn, potential mitigations to those risks.

By bringing this focus down to the cyber asset or cyber system level, you can compare your assets across all business units and locations. This methodology will make it easier to identify areas that require attention by showing you which cyber assets or cyber systems are more critical to your organization or have a lot of inherent risks. At the same time, this methodology makes it easier to see what controls have the most significant impact on reducing risk.

Armed with this detailed and nuanced information, you can make better decisions regarding where to focus your team’s limited time and money. The analysis from this type of risk assessment is valuable to managers and supervisors during the budget planning and development process. At the same time, the information in this type of risk assessment can drive value because it allows business analysts to see what assets are most critical and what threats exist to those assets, allowing those individuals to focus on the assets and threats that matter most to your organization.

-Justin Haar, Cyber Security Specialist, Minnkota Power Cooperative, and SAC Member

About the Author

Justin Haar is a Cyber Security Specialist for Minnkota Power Cooperative (MPC). In his current position, he is taking a leading role in growing MPC’s Cyber Security Program. Along with his position at MPC, Haar is also serving as a member of the MRO SAC. He has been in the IT Security industry since 2009. In that time he worked as an Information Security Consultant for small and medium-sized financial institutions. He also spent several years managing an IT Department of a mining company in northern Minnesota.

Haar received a B.S. in Computer and Network Security and an M.S. in Information Assurance from Dakota State University. He also holds several industry certifications, including the CISSP.
Supply Chain Guidance

Supply chain topics continue to make headlines in our industry. Industry guidance is available to help you with the new compliance dates, which are approaching on October 1, 2020 (Supply Chain Risk Management – CIP-005-6, CIP-010-3 and CIP-013-1). A few of the more notable sources of information are discussed below.

Let's start with webinars provided by MRO.

1. MRO Security Advisory Council (SAC) and Compliance Monitoring and Enforcement Program Advisory Council (CMEPAC) combined to sponsor a webinar on NERC Supply Chain Risk Management Requirements and Resources. This webinar was held on March 18 and covered the new requirements in CIP-013-1 and the changes to CIP-005-6 and CIP-010-3. The webinar recording is available here: https://www.mro.net/Lists/Calendar/DispForm_New.aspx?ID=411 [mro.net].

2. An Industry Coordination Group formed to improve supply chain security. This impressive partnership of industry groups includes utilities, product and service providers, industry groups, NERC committees/working groups, and third party assessors. The North American Transmission Forum (NATF) is hosting a website for the group with important information available here: https://www.natf.net/industry-initiatives/supply-chain-industry-coordination [natf.net]. The Industry Coordination Group developed a Supplier Cyber Security Assessment Model. This model was presented during a webinar on Industry Organizations’ Aligned Approach for Supply Chain Cyber Security on April 8 sponsored by the MRO SAC. The webinar recording is available here: https://www.mro.net/Lists/Calendar/DispForm_New.aspx?ID=413 [mro.net]. The overall objectives of this work and industry’s alignment were to 1) streamline common approaches to evaluating a supplier’s cyber security practices, 2) provide for flexibility within the common approaches, 3) ensure the common approaches are scalable to include all suppliers and purchasing entities, and 4) while the focus is on good cyber security practices, if executed properly, the approaches may support requirements in the NERC supply chain-related standards.

3. MRO’s SAC hosted a webinar on Third Party Vendor Review Cyber Process (Risk Management Approach) on June 16. Reviewing the cyber security posture of third party vendors and their applications is a major challenge for security departments. This webinar highlighted one utility’s approach and process for conducting reviews, pitfalls they observed, and how they developed a strategy and business case for augmenting that process.

The NERC Supply Chain Working Group (SCWG) developed several Security Guidelines based on good business practices and provided eight webinars (weekly) that concluded on May 18 on the Guidelines. The Security Guidelines can be found here: https://www.nerc.com/comm/CIPC/Pages/SCWG.aspx [nerc.com]. The webinars were recorded and will be posted as they become available.

Several other important resources discussed below are available on the Industry Coordination Group website located here: https://www.natf.net/industry-initiatives/supply-chain-industry-coordination [natf.net].

1. The NATF Supply Chain team worked with the ConEd of New York Working Group and developed a questionnaire that can be used by industry. This questionnaire is mapped to the NATF criteria and can be used by entities to evaluate supply chain risk from supplier products and services. The questionnaire contains an extensive array of questions to evaluate overall supply chain risk, and automation within the
spreadsheet to hone in on specific NATF criteria. Efficiencies can be gained by both suppliers and entities through the use of the industry questionnaire.

2. Procurement language can be difficult to craft and confusing to know where to start on a draft. Edison Electric Institute (EEI) has developed “Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk” (Version 2.0 dated May 2020), and made it available to industry. This version is EEI’s most recently updated version.

3. Vendor certifications and third party assessments can be confusing to those trying to understand the information and determine the level and quality of assurance from an independent review of a supplier or service provider. In partnership with the Industry Coordination Group, some of the nationally recognized third party assessors developed a guide to “Understanding Third-Party Assessments”.

The Supply Chain area continues to evolve as NERC has been working on a NERC Alert on Supply Chain Risk. Industry is also trying to understand the impact of the Executive Order on Securing the United States Bulk-Power System issued on May 1, 2020. Supply Chain Risk Management will be a key area for our industry as we move forward.

-Tony Eddleman, NERC Compliance Manager, NPPD, and MRO SAC Member

About the Author

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. Tony 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, Tony worked as the System Control Technology Supervisor where he managed the Energy Management System (EMS) operation and completed two major upgrade projects. He led the District’s efforts for the initial implementation of the CIP Cyber Security Standards. Tony 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.

Tony is the current chair of the NERC CIPC Supply Chain Working Group (SCWG). He is a member of the MRO Security Advisory Council (SAC), the Southwest Power Pool (SPP) Reliability Compliance Working Group (RCWG), the Reliability Team of the Large Public Power Council (LPPC) and the North American Transmission Forum (NATF) Supply Chain Steering Team.
In May, MRO hosted a Virtual CIP Conference focused on changes to certain CIP Reliability Standards and the potential impact those changes might have on MRO registered entities, along with a focused discussion of BCSI risk considerations common to the cloud environment. During one of the presentations, Brian Kinstad and Sam Chanoski, then Director of Intelligence of the E-ISAC, sat across from one another in MRO’s virtual interview booth to discuss what an attempt at compromise would look like under the FERC approved, CIP-008-6 standard that becomes effective on January 1, 2021.

Under CIP-008-6, attempts at compromise are reportable, but with the term left undefined, some have questioned what constitutes an attempt at compromise. Brian and Sam explored attempts at compromise from a pragmatic perspective, looking at hypothetical scenarios on both sides – some that warrant reporting, and some that do not.

The following exchange is an abridged transcript, taken from the full recorded interview that can be found here: https://vimeo.com/showcase/7240022 “CIP-008-6 Q&A with E-ISAC – What is an attempt?”

Questions from conference attendees and MRO’s responses are also included.

Article by Brian Kinstad, Principal Risk Assessment and Mitigation Engineer. Interview with former E-ISAC Director, Intelligence, Sam Chanoski.
Interview with the E-ISAC: Incident Response
Q&A Session Transcript

Please note that this is an abridged transcript. For an unabridged version, please reference the full recording.

Brian Q1 [5:28]: Traditionally, the E-ISAC has been focused on incident analysis and rapid sharing of security information for the electric industry. Can you provide a brief overview of the E-ISAC’s mission and how the E-ISAC engages other public and private partners?

Sam A1 [5:46]: The E-ISAC reduces cyber and physical security risk to the electricity industry across North America by providing unique insights, leadership, and collaboration. Partnerships are big part [of what we do], and cyber security is a team sport. Some partnerships have formal memorandums of understanding and program management (most of these are in the early stages). Other partnerships are based on prior interpersonal relationships that we’re looking to expand and grow out to institutionalize.

It takes two to tango, always–and we have limited resources just like everyone else–so these [relationships] sometimes move more slowly than we’d like, but that’s not necessarily related to the overall potential. But we always need to ask ourselves, “What’s in it for our members” since the E-ISAC is a member-focused organization and capability for industry. Understanding threat landscapes, and the latest vulnerabilities, and solid ways to mitigate different risks isn’t very useful if we don’t get it to those who can put the information to use.

Brian Q2 [7:43]: CIP-008-5 is the current standard requiring entities to report ‘Reportable Cyber Security Incidents’. Is CIP-008-5 the primary input for the E-ISAC today, or are incidents reported in other ways?

Sam A2 [8:00]: Not at all, in fact it’s a very small minority. Couple reasons… Most activity happens on the IT networks (further out layer of defenses), NERC jurisdiction (CIP-008) thus doesn’t apply until you get to an ESP. There are far fewer incidents in total there, and if you think of it like a pyramid, and of the small total that does occur our collective visibility is less than we’d like it to be. Can’t report an unknown.

Most information from industry comes in through voluntary information sharing, such as posts to the portal, phone calls, emails, working groups, personal relationships, and following up on media reports. There is a difference between “reporting”, which we consistently use as an indicator of a mandatory compliance obligation, versus voluntary information sharing or information exchange, which is voluntary and protected by the E-ISAC code of conduct.

Brian Q3 [9:58]: CIP-008-6 was approved by FERC in June of 2019, and will be effective January 1, 2021. One of the enhancements includes a requirement to report “attempts to compromise”. Is there any attempt too small or too insignificant to report? At what point does the E-ISAC not want to hear about an attempt?

Sam A3 [10:30]: This is the classic “getting left of BOOM” strategy. Left of boom is before the incident or catastrophe. Right of boom is the reactive after the fact recovery. We’ve all heard that defenders have to be right 100% of the time and attackers only need to be right once. This is true but incomplete. Attackers need to get every step in a long series chain of tasks right one time, and defenders have to interdict and break 100% of those attack chains in at least one place. It’s not as dire from the defense perspective. It makes
sense that the earlier that chain is broken, the less damage is going to occur.

To your specific question... Yes and no. Yes, in the sense that [insignificant] events happen in the course of humans using computers that are connected to the internet. We expect these to be automatically mitigated (this noise) by installed defenses like firewalls or IPS; your basic blocking and tackling of cyber security. That’s noise, and the sort of thing that leads to statements taken out of context like “we are attacked millions of times every day.” Well, you actually have perhaps millions of correct firewall rejections.

No in the sense that if something appears novel or interesting or significant to that organization, in the context that only they can truly understand – we want to hear about those. This is an area where humans outperform computers today, identifying anomalous anomalies, or things that “don’t look right.” Fundamentally, this is the see something, say something.

If we look at the Industrial Control Systems (ICS) Kill Chain model, based on a SANS white paper by Mike Assante and Robert Lee, that itself based on earlier IT-only Lockheed Martin Cyber Kill Chain work from the mid-2010s... this ICS Kill Chain version has two stages. The first stage is similar to what you’d see in an IT-only incident where an IT environment is compromised, data is pulled back, and things are learned. Stage two of the ICS Kill Chain talks about the activities needed to develop and test capability against an OT environment, get it back into that space, and then and actually launch an attack into ICS space.

My general professional recommendation – what I’d do if I was working for a utility today – is define an attempt as “Activity consistent with that which would take place in Stage 2 of the ICS Kill Chain” because you’ve transcended IT space to that point so you’re in scope for NERC CIP, and your observation is what would expect for the activities that are attempting to compromise your crown jewels. You can’t positively know it was an attempt without knowing the intent, and you can’t positively know intent without getting attribution, and attribution is tough and takes a long time and may never come, and is also not the most worthwhile activity for a network defender.

Brian Q4 [15:25]: The E-ISAC has a Guide for Information Sharing (September 2019) on the E-ISAC website. In the guide there are several examples of activities that may signal an attempt at compromise. Keeping in mind that most applicable systems under CIP-008-6 are already within corporate infrastructure and not directly exposed to the internet, maybe we could we review some of those activities and differentiate an attempt of interest in contrast with an attempt that has limited value to the E-ISAC?

Example Activities:

a. [16:18]: “Targeted phishing activity with a well-defined purpose”:
   i. Several individuals with higher accesses received a well-crafted phishing email

Sam [16:49]: Share, definitely. Targeted attempt that could be part of Stage 1 ICS Kill Chain (which remember is basically the same as a non-ICS related IT kill chain). Or it could be business email compromise, or any other number of things. But it’s something that is liable to cause harm to the organization, so definitely worth voluntary sharing with us.

ii. [17:17] Half of the organization received a poorly assembled phishing email with no discernable target. It may have been targeting a different industry altogether.
Sam [17:41]: Probably not worth sharing – we all get emails about pharmaceuticals, or wire transfers from Nigerian princes; those are probably noise. Exception to consider though, if it got to users’ inboxes and through your email defenses and that is a surprise, then that may be worth a share if you can safely provide an email header or other technical information to us, because it slipped through so there might be something interesting about that even though it appears random.

iii. [Not in recording - skipped for time during interview] The phishing activity seems to be industry targeted, but only a few individuals with lower risk profiles received it

[Sam’s Notes] Share, definitely, if there’s an industry tie to the theme. The most concerning adversaries know that executives know that they are frequent targets and have adjusted their behaviors some, so there has been a natural shift in victimology for social engineering efforts towards other apparently less likely targets – HR, IT staff, and engineers. Notably this is exactly what Russian actors did to gain access to a number of intermediate targets in 2016-2017 in the Palmetto Fusion campaign.

b. [18:30] “Suspicious interaction attempts against remote access systems”:

i. Evidence of a brute force authentication campaign

Sam: Sounds reportable – like an attempt to gain entry into an EACMS.

*MRO Note: The interviewer did not intend to suggest that the E-ISAC determines if incidents are reportable. The E-ISAC later confirmed on follow-up that an attempt of this nature would be useful and of interest to the E-ISAC.*

ii. [19:07] A ping passed through from the public internet to the Intermediate System. Would E-ISAC be able to analyze that and find something productive in that?

Sam: Probably not worth sharing, but look into how that passed through the perimeter firewalls and got to that intermediate system, and if that was expected and intended.

iii. [20:00] A self-propagating worm attack that targeted a security vulnerability in a popular remote desktop platform was announced on 5/14/2019. If a similar attack was observed one day after such an announcement, let’s say on 5/15/2019, would that be something that E-ISAC would find useful to have a report on?

Sam [20:30] Yes it is, and I appreciate the distinction between the actual event occurrence date and the [vendor] recognition and [announcement] date. The nature of it being self-propagating is what makes it interesting, and where it hits as a CIP-008-6 applicable system. [A report such as this] helps E-ISAC better inform the sector as a whole more quickly.

iv. [21:15] Let’s say a whole year goes by, and that same kind of self-propagating worm attack occurs again. Is an old story worth repeating? Is a report of an [older, potentially well-known compromise] such as this actionable to the E-ISAC a whole year later?

Sam: Absent from any additional specificity from the organization, probably not. This is in bounds of noise. Adversaries reuse older techniques, because they still work. It wouldn’t hurt to share it, but there is room for deference to expertise within the organization on that one.
iv. continued [22:28] Do you think from a risk perspective... is the patching date [for a vulnerability] a helpful factor in determining when the report is of use to the E-ISAC and when it is not?

Sam: [The patch date for the vulnerability] does help to add to the overall context. What part of your system did it hit? That helps us better understand and assess where the issue falls in the spectrum between benign noise and concerning activity, which helps us steer analysis and how to prioritize it.

c. [23:40] “Suspicious network traffic”

i. From a trusted partner’s environment...

Sam: Report [if applicable], [voluntary] share if not, and have a discussion with that partner

ii. [24:07] From a public source or a public destination...

Sam: Report [if applicable], [voluntary] share if not. There could be others targeted by the same activity, so a report or voluntary share helps E-ISAC determine if the attempt is an issue with one organization or the broader sector.

iii. [24:31] Suspicious network activity often brings to mind an Intrusion Detection System. MRO’s understanding is that an IDS is a tool to help entities identify interesting network traffic. With an IDS, the detections are not necessarily innocent until proven guilty, nor are they guilty until proven innocent. Do you see that the same way?

Sam: Yes - when in doubt, share [the suspicious network activity], but that said it should be with a conscious evaluation by a competent [individual], not just dump a bunch of logs and say “there’s maybe something odd in here somewhere”, that doesn’t help obviously. There is no bright line criteria here but I’d offer that if it was an observation that was fully consistent with commodity-grade malware or general risks that come with being connected to the internet, and it was validated that it was automatically blocked as designed/built/intended, that’s not particularly useful. Something that gets through [however may be of concern].

d. [25:55] “Unexplained operational technology (OT) device behavior.” Labeling this category as “unexplained” almost lands it in a cyber security incident category rather than an attempt scenario. Can you elaborate on this category? Are we looking for proof if the issue is reportable or not?

Sam: This example highlights the importance of causal analysis; it’s only unexplained until you find an explanation with enough confidence. Not always lucky enough to have a smoking gun, so this will take some effort. Let me use an analogy from the 693 reliability world: if a relay does not operate as expected, you probably wouldn’t report it for PRC-004 until you investigated the flags, looked at system topology and some oscillography, right? Same thing applies here. Proof is an elusive thing, so we’re talking more about a reasonable belief and understanding.

i. Freezes or uninitiated reboots:

MRO Note: If after an evaluation it is determined that a freeze or uninitiated reboot was due to a
cyber-security compromise, that should typically be reported as a Reportable Cyber Security Incident. Note that this would typically not be considered an attempt at compromise once attribution to an external source has been identified. The unexpected behavior would no longer be unexplained.

The End of the Reporting Obligation

Brian Q5: [28:22] The new CIP-008-6 R4 requirement indicates that three minimum attributes are required for any notification: Those being the functional impact, the attack vector used, and the level of intrusion that was achieved or attempted. Would those minimum attributes typically be sufficient to perform a complete analysis?

Sam A5: [28:40] Almost certainly not, they’re necessary but not sufficient. This is an example of the separation between the E-ISAC part and the NERC [requirements] part. [Beyond the minimum requirements, we would hope entities would not end the process there. Entities are welcomed and encouraged to continue voluntary sharing (being protected under the E-ISAC code of conduct).]

Brian Q6: [29:52] Can reports that are submitted anonymously still generate evidence of submission?

Sam A6: [30:05] It depends on the channel. A posting to the E-ISAC Portal – which can be made completely anonymously (and can be made visible to whoever the poster chooses, ranging from every registered account on the portal, to E-ISAC staff only), will generate an artifact of that post. It’s anonymous to E-ISAC, [E-ISAC] can’t see who made the posting, but that poster would have proof that can be pulled up in the future, that would be some evidence of submission. Defer to MRO on how that would assessed.

Brian Q7: [31:03] The Regional Entities (MRO) has need for quality evidence demonstrating that notification and updates to the E-ISAC are timely and include the minimum attributes. How long does it typically take E-ISAC to complete intake and analysis for a reportable attempt or an incident?

Sam A7: [31:29] Initial triage is going to be same day – that’s receiving the report, understanding it, confirming receipt if requested/based on channel, and if allowed and appropriate posting for general unattributed awareness to the Portal. During regular business hours with our full complement of analysts on it, we’re talking a couple hours. Now for the full analysis that depends on the facts and circumstances, how much information was available, and what the confidence level is. Could be same day; Ukraine 2015 took six months until we published the joint defense use case with SANS ICS.

Brian Q8: [32:38] Thinking of the three minimum attributes for CIP-008-6 Part 4.1, would the E-ISAC provide notification confirmation to the entity once the three minimum attributes have been provided?

Sam A8: [32:53] E-ISAC is not in the business of adjudicating or opining on compliance obligations. It’s safe to expect us to get to a point where we would say “we have no more questions” but there is a nuanced difference between that and a confirmation that the entity has provided the three minimum attributes. Bottom line – we will try to be helpful for obvious omissions, but the responsibility remains with the reporting entity to fulfil.
Audience Q&A

Q9: [33:58] Is an attempt considered the same as a “Reportable Cyber Security Incident”?

MRO A9: These are different things, but both are things that need to be reported.

Q10: [35:05] Is it a reportable situation with an attempt at compromise at the substation communication house that houses medium-impact BCAs (typically copper theft and related break-ins)?

MRO A10: Sometimes with a physical attack, it is hard to determine intent. Physical compromises can be diversionary and complement cyber security attacks.

Sam (E-ISAC) A10: A majority of physical attacks don’t include cyber security intent. As I understand CIP-008-6, each organization has the responsibility and the opportunity to define what an attempt is to that organization. As part of normal best practice however, performing a walk-down or check for evidence of tampering, adding, or taking away… If it’s discovered that tampering occurred related to some component of a control system, that is something that is worthy of sharing or reporting depending on how an attempt was defined.

MRO Note: As with all entity defined terms, an entity definition for attempts would also be subject to MRO professional judgement.

Q11: [38:45] Would Insider Threat investigation by entity on an employee qualify as an attempt to compromise?

MRO A11: There is no pre-qualifier category that would predetermine whether it is reportable or not. It depends on how the investigation unfolded. If this insider threat became an international espionage story you bet. That would become something MRO and E-ISAC would be interested in.

Sam (E-ISAC) A11: The fact that it’s an insider threat investigation doesn’t matter, it’s about what kind of activity is of concern and what is discovered during the course of the investigation.

Q12: [41:07] It would be beneficial for E-ISAC to explain separation with NERC if entities report matters to them.

Sam (E-ISAC) A12: The E-ISAC is a division of NERC, but within that same corporation we have the E-ISAC Code of Conduct that governs the allowable and prohibited exchange of information between the E-ISAC and NERC, and in particular the most stringent [restrictions] are about compliance monitoring and enforcement responsibilities.
MRO’s 2020 Corporate Goals
Making progress in challenging times

MRO’s board, organizational groups, and staff have shown great resiliency despite the COVID-19 pandemic, as evidenced by the great progress made on achieving board-approved annual corporate goals and metrics to support MRO’s Strategic Plan and Operating Objectives. As a reminder, the six priorities of that plan, which are also aligned with the ERO Enterprise Long-Term Strategy, are to:

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 ERO Enterprise effectiveness and efficiency
One unique attribute of MRO is that nearly all of the entities within the region participate in a Regional Transmission Organization (RTO), namely Southwest Power Pool (SPP) and Midcontinent Independent System Operator (MISO). For this reason, MRO sought to increase staff expertise this year in the area of RTO knowledge, including the role that these crucial organizations play as Reliability Coordinators and Planning Coordinators for most of MRO’s registered entities, as well as RTO markets and the linkages of those markets to achieving reliability objectives. This is reflected in MRO’s Corporate Goal 2c: “expand staffs’ depth of knowledge on RTOs and their role through training opportunities.” Through a partnership with MISO, six hours of training was provided to over 90 percent of MRO’s staff throughout May and June regarding RTOs. I’d like to personally thank MISO staff for their generous commitment of time, and in particular Senior Director of Regional Operations David Zwergel, who helped coordinate this effort. MRO is currently exploring similar opportunities with SPP, to include WECC staff due to SPP’s recently expanded role in the Western Interconnection.

In 2018 and 2019, MRO Principal Technical Advisor John Seidel and I were part of a FERC/ERO inquiry team that analyzed a cold-weather event that took place in our footprint. The findings from that inquiry identified some emerging reliability risks and were communicated in a report to industry, in addition to a number of outreach events across North America. MRO’s 2020 Regional Risk Assessment also discussed a number of the key findings in our region that helped shape MRO’s 2020 activities. Throughout this year, MRO has made progress on addressing a number of these emerging risks. Examples include more depth in staff’s review of Facility Ratings through compliance activities, efforts of the MRO NERC Standards Review Forum (NSRF) to contribute to the Standards Authorization Request that was submitted by SPP for the development of a Reliability Standard to enhance reliability during cold-weather events, and the development of a MRO cold-weather generation preparedness program through collaboration with ReliabilityFirst. This new outreach program will be implemented by MRO’s RAPA department outside of any CMIE activities. Russ Mountjoy is leading the development of this program and has an article introducing it in this newsletter on page 29.

Due to the COVID-19 pandemic, MRO is not planning any generator site visits this year related to the new program. The MRO Board approved that change to MRO’s 2020 metrics at its second quarter meeting, which has been the only change made to MRO’s 2020 metrics thus far.

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
LATEST NEWS:

**FERC Commissioner Bernard L. McNamee Announces Departure**

On August 5, 2020, Commissioner McNamee announced his departure from the Commission. Read his full statement.

**FERC, NERC Publish Guide to Identify Supply Chain Vendors**

FERC and NERC took a further step to protect the nation’s electric infrastructure today by publishing a joint white paper to help the electric sector identify vendors of components on their networks so that they can take any necessary action to mitigate potential risks to the bulk power system. Read the full announcement.

**Grid Demonstrates Improved System Performance and Resilience in 2019**

In the face of rapid, significant changes to the generation resource mix, the bulk power system continued to perform at a very high level of reliability in 2019, NERC’s 2020 State of Reliability found. Performance trends for generation and transmission as well as protection and control measures are positive, and metrics showed improvement in numerous areas. With appropriate insight, careful planning and continued support, the sector will continue to navigate the challenges in a manner that maintains reliability. Read the full announcement.

**NERC Posts Reference Materials**

In collaboration with National Institute of Standards and Technology (NIST) staff, NERC staff assessed and updated the reference document mapping NERC Critical Infrastructure Protection (CIP) Reliability Standards to the NIST Cybersecurity Framework (the Framework). The previous version of the mapping referenced now-retired NERC CIP Reliability Standards and a previous version of the Framework.

INDUSTRY EVENTS:

**ReliabilityFirst’s Sixth Annual Protection System Workshop for Technical Personnel**

August 18 | 7:00 - 11:00 am EST | WebEx

This Protection System Workshop for Technical Personnel will cover a diverse range of topics and discussions relative to Protection Systems tailored to the needs of technical personnel and will include speakers from RF, industry subject matter experts, and others. Topics slated for discussion include capacitor bank protection, protection simplicity, and IEC 61850 regarding communication in substations. Register here.

**ReliabilityFirst’s Human Performance Improvement Overview**

August 19 | 7:00 - 11:00 am EST | WebEx

New for 2020, there will be a half-day session on the morning of August 19 for a Human Performance Improvement (HPI) Overview by Dr. Jake Mazulewicz. This overview session is intended for those that are new to the human performance arena or who just want to refresh their knowledge of human performance principles and concepts. Register here.

This overview is followed by the Third Annual Human Performance Conference on Thursday, August 20 from 7-11 am EST. Register here.

**NERC Board of Trustees Meetings**

August 19-20 | WebEx

For more information and to register, click here.

**RF 2020 Fall Virtual Workshop**

August 25 | 7:00 - 4:00 pm EST | WebEx

This workshop will focus on Facility Ratings. In addition to addressing FAC-008 updates to the NERC CMEP Practice Guide, the agenda includes topics ranging from validation and verification to the commissioning process to internal controls. For more information and to register, click here.
Industry Workshop: Project 2016-02 Modifications to CIP Standards - Virtualization
August 27 | 12:00 - 5:00 pm EST | WebEx
Register here.

Industry Webinar: Winter Preparation for Severe Cold Weather
September 3 | 2:00 - 3:00 pm EST | WebEx
Register here.

ERCOT and Texas RE Generator Weatherization Workshop
September 3 | 8:00 - 12:00 CST | WebEx
See the full agenda and register here.

Monitoring and Situational Awareness Technical Conference - Session 1
Sept 24, Oct 15, Nov 10 | WebEx
NERC will host its eighth annual Monitoring and Situational Awareness Technical Conference via Webex. The theme of this year’s conference is “Energy Management System Reliability and Resiliency in the Pandemic.” This year’s conference will unite expertise from various utilities to share cutting-edge ideas and good industry practices, and to identify trends and lessons learned from events across different vendors, energy management system (EMS) platforms, and interconnections. There will be three (3) different conference sessions to choose from: Register here.

CANCELED: NERC GridSecCon
October 20-23, 2020 | Houston, TX
NERC’s Electricity Information Sharing and Analysis Center (E-ISAC) and Texas Reliability Entity have cancelled GridSecCon 2020. The conference, originally planned for October 20–23 in Houston, Texas, will resume in October 2021.

REGIONAL AND MRO EVENTS:

MRO Cyber Asset Management Webinar
August 20 | 10:00 - 11:00 am CST | WebEx
MRO’s Security Advisory Council is hosting a webinar on Cyber Asset Management. This webinar will explore tools and techniques that can assist in asset discovery, identification, and asset management. The goal is to provide individuals with knowledge and tools to start identifying, categorizing, and classifying assets on their network. This in turn is a key requirement for asset management, risk management, and vulnerability management. Register here.

MRO Reliability Advisory Council Meeting
August 25, 2020 | 8:00 - 3:00 CST | WebEx
For the full meeting agenda and registration, click here.

MRO Virtual Reliability Conference
August 26, 2020 | 9:00 - 3:00 CST | WebEx
The purpose of this conference is to provide registered entities valuable information for technical staff, subject matter experts, and power system engineers and any other interested industry partners. There is no fee for attendance. See the draft agenda. Register here.

MRO CMEP Advisory Council Meeting
September 16, 2020 | WebEx
See the full meeting agenda and register here.

MRO Board and Board Committee Meetings
September 16-17, 2020 | WebEx
MRO’s Board of Directors and its Governance and Personnel and Organizational Group Oversight Committees meet next on September 16-17, 2020, by WebEx. More information on these meetings is available on MRO’s website calendar.

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.