The Benefits of Risk-Based Regulation
Sara Patrick, President and CEO

When I first joined MRO in August 2008, reliability regulation of the very complex and interconnected bulk power system was in its infancy. FERC had just issued its first Notice of Penalty Order on July 3, 2008, and in it provided some pretty lengthy direction on what to include in enforcement determinations going forward. Fast-forward ten years and regulation looks significantly different. The last decade has seen a maturation of ERO Enterprise (ERO) thoughts and processes as we learn to focus more on, and address critical risks. As an early supporter of risk-based regulation, I am incredibly fortunate to have been a part of this process from the beginning, to have watched our risk-based philosophy evolve, and to have helped nurture it through as it matures.

Today, our regional risk assessment, entity inherent risk assessments, and compliance oversight plans reflect how we carefully consider risk in our oversight work. With the implementation of these risk-based oversight tools, compliance monitoring is tailored to each registered entity and more focused on the risks that can impact reliability. Our enforcement processes too, have evolved to be more proportionate to the risk a noncompliance poses to system reliability. FERC and our Canadian regulators in Manitoba and Saskatchewan now allow the ERO to exercise more discretion based on risk, and we have fully embraced and continue to implement streamlined processing methods, such as compliance exceptions and self-logging. With these new alternatives to enforcement, self-reporting has increased and settlements are rare.

These risk-based programs began as pilot projects just a few short years ago, and have developed into the risk-based compliance monitoring and enforcement approach the ERO uses today. The benefit of this risk-based oversight approach is paying real dividends—both for the ERO and for industry. MRO developed the Compliance Severity Index (CSI) and the Event Severity Index (ESI) that evaluate the region’s progress toward the ERO’s metrics of fewer, less severe events and fewer, less severe violations. The CSI represents the total risk that all instances of noncompliance present to the reliability and/or security of the bulk power (Continued on page 2)
system in the MRO region. MRO undertakes a rigorous process to evaluate each instance of non-compliance, based upon an analysis of the specific facts and circumstances, to determine the potential and actual risk to the reliability and/or security of the bulk power system. The result of this process is a risk determination with an assigned risk level of minimal, moderate, or serious. MRO uses the risk determination and discovery method to calculate the CSI.

The CSI shows a trend towards less severe violations in the MRO region. While MRO has seen an increase in the number of noncompliances identified, the vast majority of those issues are self-reported minimal risk issues. MRO also tracks any repeat violations within one year of a previous moderate or serious risk violation. There have been no such repeat violations in the past four years. There is also a very positive trend in the MRO region with entities accepting responsibility and mitigating noncompliances quickly and completely.

Similarly, MRO’s ESI measures the severity and frequency of events on the regional bulk power system. All events in the MRO region over the past eight years have been category 2 or lower events. Consistent with High Reliability Organization theory, finding and fixing small errors helps prevent large scale, cascading events.

MRO’s CSI and ESI validate that risk-based regulation delivers real results—improving reliability of the regional bulk power system. With the implementation of risk-based compliance monitoring, MRO auditors are having more in depth discussions with entities focused on ensuring reliabil-

---

**MRO Compliance Severity Index**

---

<table>
<thead>
<tr>
<th>Year</th>
<th># Events</th>
<th>Category 0</th>
<th>Category 1</th>
<th>Category 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011</td>
<td>17</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td>5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2013</td>
<td>11</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2014</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2015</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2016</td>
<td>15</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2017</td>
<td>13</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2018</td>
<td>5</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Year</th>
<th>Total BPS Impact &amp; Average Impact by Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011</td>
<td>38</td>
</tr>
<tr>
<td>2012</td>
<td>56</td>
</tr>
<tr>
<td>2013</td>
<td>95</td>
</tr>
<tr>
<td>2014</td>
<td>110</td>
</tr>
<tr>
<td>2015</td>
<td>14</td>
</tr>
<tr>
<td>2016</td>
<td>88</td>
</tr>
<tr>
<td>2017</td>
<td>62</td>
</tr>
<tr>
<td>2018</td>
<td>38</td>
</tr>
</tbody>
</table>

---

**MRO Event Severity Index**

---

**Average BPS Impact/Event**

---

<table>
<thead>
<tr>
<th>Category 0</th>
<th>Category 1</th>
<th>Category 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011</td>
<td>89</td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td>56</td>
<td></td>
</tr>
<tr>
<td>2013</td>
<td>95</td>
<td></td>
</tr>
<tr>
<td>2014</td>
<td>110</td>
<td></td>
</tr>
<tr>
<td>2015</td>
<td>34</td>
<td></td>
</tr>
<tr>
<td>2016</td>
<td>88</td>
<td></td>
</tr>
<tr>
<td>2017</td>
<td>62</td>
<td></td>
</tr>
<tr>
<td>2018</td>
<td>38</td>
<td></td>
</tr>
</tbody>
</table>
ity and implementing management practices around reliability and security of the bulk power system, which will continue to drive results.

Back in April, I joined several ERO colleagues on a “CEO Panel” at American Electric Power’s (AEP) internal Compliance Summit. Nick Akins, AEP’s CEO, inquired about the apparent emphasis on enforcement. In response, I shared my view that enforcement is just one of the tools in our toolbox. It is not the largest tool and it is not the first tool we reach for. As a risk-based regulator, we have several tools at our disposal to promote reliability and deter noncompliance. There are many ways outside of imposing financial penalties where we can help an entity conform to the requirements and be a Highly Effective Reliability Organization (or HERO™).

As I see it, the greatest, most effective tool we have to preempt noncompliance is outreach—providing clarity on the requirements and sharing lessons learned and industry best practices throughout the region. In recent years, NERC and the Regions have significantly expanded outreach efforts. At MRO, we have worked to promote a greater understanding of the rules; effectively communicate our expectations; provide information and guidance where appropriate; build constructive, ongoing relationships with those we regulate; and be a respected resource for industry participants.

So far in 2018, MRO has conducted six webinars and conferences for the purpose of providing information to industry on the threats and risks that could potentially impact reliability of our regional bulk power system. Our annual Security Conference is planned for September 26, and will focus on expanding the security awareness and strengthening the cybersecurity and physical security posture of entities registered in MRO through information sharing by experts within the security industry. The day prior to the conference, MRO is hosting security training for entities registered in the MRO region. The training will focus on physical security (drones & explosives) and cybersecurity incidents.

We also have a fall Reliability Conference and our annual CMEP Conference planned later this year. Visit the MRO Calendar for more information on these events.

MRO is invested in, and deeply committed to improving and expanding the ERO’s risk-based philosophy, which includes a strong focus on outreach and education.

I welcome your comments and ideas at sara.patrick@mro.net.

Our future is bright!
ERE Enterprise Program Alignment Process

Supporting Efforts For Appropriate Alignment across the ERO Enterprise

Introduction

In August 2017, NERC introduced the Electric Reliability Organization (ERO) Enterprise Program Alignment process, which supports efforts for appropriate alignment in the ERO Enterprise execution of both the Compliance Monitoring and Enforcement Program (CMEP) and the Organization Registration and Certification Program (ORCP).

Through collaboration among NERC, the Regional Entities (REs), and the Compliance and Certification Committee (CCC), this program has been in place for the past year.

This presentation is intended to address the program’s progress during its initial implementation year, focusing on outreach efforts, an update on submitted and resolved cases, and early observations.

Background

The ERO Enterprise is focused on continuous improvement and alignment of CMEP and ORCP activities. Greater alignment across the ERO Enterprise ensures effective and efficient use of resources, and it allows stakeholders to maximize focus on the most significant risks to reliability. While implementation of the risk-based CMEP and related oversight activities have promoted a greater degree of alignment in enforcement and compliance monitoring activities, the Program Alignment process further helps to identify new approaches to consistency and to leverage ongoing efforts across the ERO Enterprise.

The CCC also has a role in framing issues for the ERO Enterprise to consider when planning its Program Alignment activities. NERC and the CCC have been working together over the last year to inform industry about the program and how stakeholders can help in their reporting. In 2017, the CCC formally established a CCC Alignment Working Group (AWG) responsible for executing the CCC’s role within the process. For example, the AWG has helped to provide the ERO Enterprise with more detail or context to understand better certain anonymous submissions, and its members have also participated directly in stakeholder outreach during NERC and RE conferences.

To assist registered entities in understanding where acceptable differences exist and to increase overall transparency across the ERO Enterprise, NERC – with the support of the REs – has developed the Regional Program Information Matrix. To inform the Regional Program Information Matrix, the ERO Enterprise gathered and consolidated a description of regional processes for program areas such as CMEP implementation, ORCP, and Self-Logging.¹

¹ NERC Rules of Procedure and ERO Enterprise guidance are the governing documents. Any differences in regional processes should not cause material effects on ERO Enterprise programs and should support the fair and reasonable treatment of registered entities.

(Continued on page 5)
Also in 2017, NERC implemented the Consistency Reporting Tool using a third-party vendor, which allows stakeholders to submit consistency issues anonymously, if desired. NERC’s Consistency Reporting Tool replaced the Regional Consistency Process and Tool. This tool has been the primary source of new cases provided through the program thus far in 2018.

The ERO Enterprise Program Alignment Process web page also launched in 2017. This web page provides industry information on the CMEP Alignment process, the CCC AWG’s participation, a link to the Consistency Reporting Tool, and other resources and reference documents.

The web page provides transparency on issues the ERO Enterprise has received and the recommendations or resolutions of those issues through a regularly updated Issues and Recommendations Tracking spreadsheet.

**Program Alignment Progress**

Since launching, the ERO Enterprise Program Alignment Process has identified 18 issues for consideration. Of those issues, 12 have been completed. The ERO Enterprise is still in the process of addressing six issues. Of those six issues, registered entities submitted two to NERC directly or via the Consistency Reporting Tool. There are also four issues of a more complicated nature that NERC Compliance and Enforcement identified in 2017 related to CMEP processes that have multiple stages toward resolution. The current status of all issues is described in the Issues and Recommendations tracking spreadsheet.

**Program Alignment Outreach**

Stakeholder outreach and information sharing on the Program Alignment efforts remain key priorities of the ERO Enterprise and the AWG, and there have been several targeted efforts since launching in August of 2017 to support stakeholder awareness of the program. Notably, ERO Enterprise staff and AWG members have provided information to stakeholders on the program, how to submit an issue, and where to find additional resources in the following ways:

- Standards and Compliance Workshop in July 2018,
- At most Regional Entity workshops in the fall of 2017 and spring of 2018,
- At various forum and trade association meetings,
- Through a Program Alignment industry webinar in October 2017,
- Through updates in NERC news, and
- By adding a permanent link to Program Alignment and the Consistency Reporting Tool in the weekly bulletin, along with noting key developments as issues are resolved.

**Program Alignment Early Observations**

In the last year, both the ERO Enterprise and the CCC have noted some early successes in the process and outreach efforts. NERC is also seeing more cases submitted to the program by stakeholders, as summarized in Table 1 above, which has provided an opportunity to resolve quickly perceived or actual alignment issues, particularly those related to common understanding of CMEP practices.

NERC has received feedback on the program itself and has made appropriate enhancements related to ensuring the effective and efficient tracking of issues, the triage process leveraging the REs and the AWG to prioritize activities, and providing the appropriate level of transparency through reporting and the NERC website.

<table>
<thead>
<tr>
<th>Table 1: Issues by Source</th>
<th>2017</th>
<th>2018</th>
<th>Completed</th>
<th>In Progress</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regional Consistency Reporting Tool (now closed)</td>
<td>2</td>
<td>n/a</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Consistency Reporting Tool (launched August 2017)</td>
<td>3</td>
<td>3</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>NERC</td>
<td>7</td>
<td>1</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Stakeholder</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Total*</td>
<td>12</td>
<td>6</td>
<td>12</td>
<td>6</td>
</tr>
</tbody>
</table>

*As of June 22
Richard Burt Appointed Senior Vice President and Chief Operating Officer

In August, MRO’s Vice President Risk Assessment, Mitigation and Standards Richard Burt was promoted to Senior Vice President and Chief Operating Officer, reporting to President and CEO Sara Patrick. In his new role, Burt will oversee and be responsible for providing strategic direction and guidance to MRO’s compliance monitoring, risk assessment and mitigation, registration, security and operations teams.

“Richard’s many years of industry experience, diverse technical power systems background, and exemplary leadership skills have been instrumental to MRO’s success,” said Patrick. “He is uniquely qualified to oversee MRO’s technical teams and I am confident that he will continue to drive operational excellence across these areas of the company and help lead alignment efforts within the ERO.”

Burt joined MRO in February 2012 as a Principal Risk Assessment and Mitigation Engineer and was promoted to Vice President Risk Assessment, Mitigation and Standards in April 2015. About the promotion, Burt said “I’m honored to have the opportunity to lead the diversely talented technical staff that comprise these teams at MRO, and look forward to furthering collaboration in support of effective and efficient mitigation of reliability and security risks to the bulk power system.”

MRO Vice President Operations Dan Schoenecker Announces Plans to Retire

MRO’s Vice President Operations Dan Schoenecker has announced he will retire at the end of 2018. Schoenecker has served as Vice President Operations for the past 12 years and the organization has certainly benefited from his many years of industry experience, knowledge of the regional bulk power system, and leadership in many areas of the company. Schoenecker also represented MRO on many NERC and ERO leadership teams, along with industry committees and working groups.

“Dan’s highest priority has always been reliability of the bulk power system,” Patrick said, “He has been an instrumental member of the MRO team and we are really going to miss him.” Schoenecker will begin his transition immediately and will be in the office three days a week.

New Directors Appointed To Oversee Day-to-Day Operations

Two new director-level positions have been created and filled internally to oversee the activities of MRO’s compliance monitoring and risk assessment and mitigation teams. Reporting directly to Burt, these new director positions will ensure greater alignment in the application of the standards and in the risk-based oversight tools used by MRO to identify and mitigate risks to reliability of the bulk power system.

Jeff Norman Promoted to Director of Compliance Monitoring

Jeff Norman joined MRO in January 2012 as a Senior Compliance Engineer, in 2014 transitioned to the role of Senior Risk Assessment and Mitigation Engineer, in 2017 was promoted to Risk Assessment and Mitigation Principal, and in August 2018 was named the Director of Compliance Monitoring.

Prior to joining MRO, Norman worked as a Transmission Planning Engineering Consultant and as a Transmission Planning Engineer for both Power System Engineering and Excel Engineering. He also worked for MAPPCOR as a Student Engineer.

Norman attended the University of Minnesota where he earned a Bachelor of Science degree in Electrical Engineering in 2002 and then earned a Mas-
William Steiner Promoted to Director of Risk Assessment and Mitigation

William Steiner joined MRO in February 2013 as Risk Assessment and Mitigation Principal. He was promoted in August 2018 to Director of Risk Assessment and Mitigation.

Steiner has over 30 years of experience working with electric utilities. Prior to working at MRO, he worked at Siemens Energy Automation as a project and software development Manager, Xcel Energy as Manager of the EMS, Open System International as System Engineering Manager of the Monarch EMS platform, and at Washington Water Power (now Avista Corp) as a Senior Engineer performing transmission planning studies and supporting the EMS. Steiner also worked as a Distribution Engineer at Public Service Company of New Hampshire.

Steiner attended Drexel University, where he earned a Bachelor of Science degree in Electrical Engineering specializing in Power and Machines. He holds the Certified Information Systems Security Professional (CISSP) and Project Management Professional (PMP) Certifications.

Ken Gartner Promoted to Director of Internal Oversight and Information Technology

Ken Gartner joined MRO in April 2011 as a CIP Audit Specialist and was promoted to Compliance Monitoring and Enforcement Program (CMEP) Process Principal in August 2013. In September 2018, he was promoted to Director of Internal Oversight and Information Technology.

In this new position, Gartner will be responsible for conducting and directing periodic internal oversight monitoring of MRO’s CMEP activities, facilitating responses to all NERC and FERC oversight requests related to delegated functions (excluding financial oversight requests), and overseeing MRO’s Information Technology Department operations. Gartner will report to Sara Patrick.

Prior to joining MRO, Gartner held positions at 3M Company, Ernst & Young LLP (E&Y), Data Recognition Corporation (DRC), and Computer Sciences Corporation (CSC). His roles included leading and performing information technology and compliance audits, independent attestations, physical security and system implementation reviews, project consulting, and systems analysis. Mr. Gartner has experience working in a variety of regulated industries and within both large and small companies.

Gartner attended the University of Minnesota Carlson School of Management, where he earned a bachelor degree in Accounting, Management, and Marketing. He has an active Certified Public Accountant (CPA) License in the state of Minnesota and holds the Certified Information System Security Professional (CISSP), Certified Information System Auditor (CISA) and Certified in Risk and Information Systems Control (CRISC) certifications.

About the new organizational structure, Patrick said, “This new structure better aligns MRO with the ERO Enterprise and allows us to more effectively and efficiently implement and expand our risk-based approach to regulation. I am looking forward to the leadership, insight and experience these new directors will bring both to MRO and the ERO.”

Please join us in congratulating these individuals on their achievements!
FINANCE AND ADMINISTRATION

Sue Clarke, Vice President Finance and Administration

MRO Year-to-Date Financials

Year-to-date unaudited actual expenses for the FERC-approved 2018 budget were 5 percent over. Staff anticipate budget will be met within +/- 5 percent by year-end. Additionally, a projected $1.8M will be expended by year-end due to the SPP RE transition. These transition costs will be funded through a transfer of SPP RE assessments.

2019 Business Plan and Budget

The NERC Board of Trustees approved the Regional Entity business plans and budgets on August 16, 2018. Comparatively, the 2019 MRO budget reflects an assessment increase of 44 percent over the 2018 approved budget, but will experience a savings or reduction per Net Energy for Load (NEL) charged to load-serving entities throughout the new geographical area.

The 2019 budget is sufficient for MRO to meet its delegated responsibilities. NERC filed the NERC and seven Regional Entity budgets with FERC on August 24, 2018. FERC approval typically occurs in October or November.

Culture and Talent Management

Activities related to the SPP RE transition continue to progress with 9 out of 12 open positions being filled. Recruitment efforts continue as candidates are identified for the remaining open roles. In addition to the planned SPP RE transition roles, two other positions are now filled: Security Administrator and Director of Human Resources.

The addition of staff has allowed for several meet and greet activities to take place, which have created opportunities for staff to welcome new team members and also allowed for more broad team interactions to occur. MRO also coordinated a welcome conference with the new SPP RE entities, which gave staff and entities an opportunity to meet and understand the new MRO Region. Additional team building activities included an opportunity for staff (and families) to volunteer at the Little Farm Hands activity booth at the Minnesota State Fair the end of August, as well as an all staff team building off-site activity scheduled in September.

Staff training has been scheduled for the fourth quarter. Staff will complete a virtual harassment prevention and employee conduct training requirement. Staff will also participate in an Advance Error Reductions workshop facilitated by Fisher Improvement Technologies. The facilitator has worked with other Regions and NERC on this same subject.

Any questions related to the business plan and budget, accounts and/or talent management can be directed to Sue Clarke, VP of Finance and Administration.

All successful people have a goal. Not a fuzzy, indefinite objective, but a sharp, clearly defined, specific goal. No one can get anywhere unless he knows where he wants to go and what he wants to be or do.

-Norman Vincent Peale, writer and minister
Security-Related Webinars Hosted By MRO’s Security Advisory Council

The MRO Security Advisory Council (MRO SAC) is an organizational group that provides advice and counsel to MRO’s Board of Directors, staff, members and registered entities regarding: (1) cybersecurity; (2) physical security; and (3) SCADA, EMS, substation and generation control systems. The MRO SAC serves as topical experts that identify and monitor risks and share information on security-related issues across the region.

To facilitate this information sharing, the MRO SAC hosts several webinars throughout the year on security topics. Most of these webinars are recorded and can be found on the MRO SAC Home Page.

The MRO SAC encourages you to review past webinars and register for future webinars as they become available. Upcoming webinars can be viewed here.

Below is a list of webinars that have been hosted by the MRO SAC:

Exploring the Unknown ICS Landscape:

(Not Recorded.) This webinar provided a discussion regarding unique research on industrial control system software, malware, and the consequences of poor operations security. The premise for this project is the belief that there is a wealth of information surrounding Industrial Control Systems that is unrecognized by the traditional IT cybersecurity industry. Robert M. Lee, CEO of Dragos, walked through proven methodology and showed real-world findings and conclusions of what this means in our space.

GridEx IV: Benefits of Participation:

(Recorded.) This webinar provided guidance on utility company participation in NERC’s biennial grid security exercise, GridEx IV. GridEx provides an opportunity for utilities to demonstrate their abilities to respond and recover from a simulated coordinated cyber and physical attack on the bulk electric system.

Intelligence 101: Establishing and Maturing an Effective Threat Intelligence Program:

(Recorded.) This webinar provided a common understanding of security and risk intelligence, discussed the foundational aspects of an intelligence program, and explored the use cases that can be implemented to establish or mature intelligence functions without requiring complex projects or expensive feeds.

Physical Security Assessment:

(Recorded-please email Estee Kolles for webinar link.) This webinar provided an in depth look at the DHS IST tool and a brief overview of a similar tool used by Public Safety Canada.

GridEx Lessons Learned:

(Recorded.) This webinar provided lessons learned from NERC’s biennial grid security exercise GridEx. GridEx is designed to simulate a cyber/physical attack on electric and other critical infrastructures across North America. This hour-long webinar was presented by representatives from a diverse group of entities, including a small vertically-integrated utility (Lincoln Electric System), a Regional Transmission Organization (Southwest Power Pool) and two government agencies (Department of Homeland Security and North Dakota Emergency Services).

If you have any ideas for future MRO SAC-hosted webinars, please don’t hesitate to let us know by emailing Estee Kolles, Security Administrator, and/or filling out the online webinar request form: MRO Security Advisory Council (SAC) Webinar Request Form.

To be added to the MRO SAC Plus email distribution list to receive future MRO SAC-hosted webinar notifications, please email Estee Kolles, Security Administrator.
The MRO Security Advisory Council (SAC) is pleased to announce the fifth annual Security Conference at MRO’s office in Saint Paul, Minnesota. The conference will be preceded by a day of technical training on cybersecurity and physical security that is now sold-out, however, you can be added to the waitlist and if seats become available you will be contacted. The training will be followed by an evening social networking event for all technical training and conference attendees. Security professionals, subject matter experts, and power system engineers from registered entities in the MRO Region are encouraged to attend.

Technical Training September 25, 2018 | 8:00 a.m. to 3:30 p.m.
This technical training provides security education to registered entities in the MRO Region. Agenda Topics:

- Physical Security (Drones & Explosives) – The drone session will feature an up to date review of how drones are being used in the electric sector and the pitfalls and benefits of drone technology. The explosives session will include examples of improvised explosives and insight into how to prepare, respond, and investigate incidents involving the use of these devices.
- Cybersecurity (Hands on Incident Handling Lab) – This workshop provides fundamental skills to handle and respond to cybersecurity incidents. Laptops are required for this training and will not be provided.

To add your name to the ‘wait-list’ to attend the technical training click here. Space is limited to 100 people and the ‘wait-list’ closes on September 18, 2018.

Social Networking Event September 25, 2018 | 5:00 p.m. to 7:00 p.m.
This social networking event allows attendees to meet in a relaxed setting and enjoy appetizers at the Hampton Inn & Suites, 200 7th Street West, Saint Paul, Minnesota, 55102. When registering for the Security Conference and/or the Technical Training, please check the box if you will also be attending the social networking event.

Security Conference September 26, 2018 | 8:00 a.m. to 4:30 p.m.
This conference is designed to provide clarity by expanding security awareness and strengthening cybersecurity and physical security through information and training shared by experts within the security industry, as well as analysis of real world security lessons and best practices. Due to the nature of this conference, there will be limited in-person attendance available. The conference will also be live-streamed via WebEx. Agenda Topics:

- Electricity Subsector Coordinating Council (ESCC) – Kevin G. Wailes, Lincoln Electric
- Electricity Information Sharing and Analysis Center (E-ISAC) – Bill Lawrence, E-ISAC
- Executive Security Perspectives – Steve Brown, Xcel Energy and Keri Glitch, MISO
- Physical Security – John Breckenridge, KCP&L
- Cybersecurity – Christophe Veltsos, Minnesota State University, Mankato

To register to attend the Security Conference either in-person or via WebEx, click here. Registration closes on September 18, 2018.

Questions on this conference can be sent to Estee Kolles, Security Administrator.
Jessie Mitchell, Stakeholder Relations and Communications Principal

On August 13, 2018, the West Virginia House of Delegates voted to impeach all four sitting justices of the West Virginia Supreme Court of Appeals. The reason for the impeachment? Lavish spending, lying, cheating, and fraud are just a few.

The judges are Chief Justice Margaret Workman and Justices Allen Loughry, Elizabeth Walker and Robin Davis. According to National Public Radio (NPR), Workman, Loughry and Walker are now facing impeachment trials in the state Senate, while Davis announced her retirement immediately after the impeachment. A fifth judge, Justice Menis Ketchum, retired in July before the impeachment proceedings began. He has since pled guilty to one count of federal wire fraud and faces up to 20 years in prison.

Impeachment charges for the four justices range from personal use of state-owned vehicles and computers to failing to carry out administrative duties. Loughry, Workman and Davis were also impeached for paying retired senior status judges more than the law allowed, and Loughry and Davis were impeached for failing to control office expenses—they spent $363,000 and $500,000 respectively on office renovations. Loughry is also accused of keeping a $42,000 antique desk and $32,000 suede couch at his home. Walker and Workman spent hefty sums on office renovations too (just over $100,000), but were not impeached on those charges.

According to NPR, the House Judiciary Committee “approved 14 articles of impeachment against the four judges, accusing them of ‘maladministration, corruption, incompetence, neglect of duty.’”

The West Virginia Supreme Court of Appeals website states that the five Supreme Court justices are elected in nonpartisan elections to twelve-year terms. The West Virginia Governor appoints justices to fill vacancies. An appointee who wishes to remain in office to fill the unexpired term must run in the next general election. NBC News reports on the partisan debate that has ensued over the scandal. Politics aside, the unprecedented action of the West Virginia state legislature has left the state without a functioning Supreme Court.

Periodically, MRO staff participates in ethics training with Charles Selcer, managing partner at the Minneapolis firm Schechter Dokken Kanter. Selcer teaches Professional Ethics classes for the Minnesota and North Dakota Society of CPA’s and for CPA firms and universities across the country.

During these training sessions, Selcer reviews real-life ethics cases and uses these examples to identify ways to improve ethical decision-making.

“If the work you do is noble and legal, then there must be an inherently ethical way of discharging it, whether by written code or not.”

- Charles Selcer, CPA

(Continued on page 12)
throughout the course of everyday work. Some of the examples provided by Selcer are clear indications of unethical behavior, while others make ethics violations much harder to spot.

Selcer teaches us that unethical behavior can erode public trust and disrupt the orderly functioning of commerce. He also reminds us that good people can do bad things, and will justify their behavior as “not that bad.” Selcer suggests that one always consider what a third-party outsider would think looking in. How would a particular behavior or action appear to that person?

In the case of the West Virginia Supreme Court, an outside perspective would suggest that a $500,000 office remodel is over the top and indicates wasteful spending and misappropriation of taxpayer dollars. On the other hand, using a company vehicle or laptop for personal use may seem easier to rationalize depending on the context.

The lesson learned here? No matter the infraction, taking advantage of one’s position or authority for personal gain is never wise. Especially for a judge.

Jessie Mitchell, Stakeholder Relations and Communications Principal

Over the past several years, you have likely heard or read something from MRO promoting High Reliability Organization (HRO) theory. HROs are organizations that have succeeded in avoiding catastrophes in environments where accidents can be expected due to complexity, interdependence, and risk. Over time, HRO theory has evolved and provides guidance for modern safety program design and is foundational to many industries seeking high reliability in critical functions.

Karl Weick and Kathleen Sutcliffe articulate in their book, Managing the Unexpected: Assuring High Performance in an Age of Complexity, how HROs follow five overarching principles: 1) Preoccupation with failure, 2) Reluctance to simplify, 3) Sensitivity to operations, 4) Commitment to resilience, and 5) Deference to expertise.

These five principles are fundamental and are the basis of improvements in quality, reliability, productivity, and resiliency in any organization. Organizations that have these qualities produce a collective state of mindfulness. To be mindful is to have a rich awareness and a discriminatory sense of detail, which enhances the ability to discover and correct errors before the errors compound and escalate into a crisis. By developing mindfulness, HROs demonstrate the capacity to anticipate and to contain unexpected problems. In our industry, Highly Effective Reliability Organizations™ (or HEROs) keep the small stuff small and prevent uncontrolled, cascading events.

This is why the HRO theory is the perfect framework for implementing the high standards of operational excellence needed to support the ERO Enterprise vision of “A highly reliable and secure North American bulk power system.” Taking this concept a step further, MRO translated the HRO theory in its Mission statement, which is "to identify, prioritize and assure effective and efficient mitigation of risks to the reliability and security of the North American bulk power system by promoting HEROs."

There are several ways in which MRO supports and promotes HEROs. For example, we provide Clarity to industry on the regulatory requirements through technical reports, Standard Application Guides, and training and education events. We also share information and lessons learned from compliance monitoring activities and system events through newsletter articles and other outreach efforts. You can read more about how our work supports HEROs in Sara Patrick’s article on the benefits of risk-based regulation.

So how do you know if your organization is a HERO?

In 2011, MRO adapted a HERO Survey that allows companies to assess how well they implement several activities that support the five HRO principles. The survey results inform respondents of where they are highly effective and reliable, and where work remains to be done. The survey results are returned to the individual completing the survey, and not shared with MRO. The survey can be downloaded from our website and shared across your organization. You can take the survey now, and then take it again after implementing changes based on the survey results.

The survey is an excellent tool to strengthen awareness and build a capacity for mindfulness within your organization—we encourage you to take it!
Standards Efficiency Review Update

The Standards Efficiency Review (SER) project was initiated by the ERO Enterprise to reduce the compliance burden on registered entities through the elimination of requirements determined to provide minimal benefit to the reliability of the bulk power system. This is the largest initiative of this nature since NERC addressed paragraph 81 of FERC’s March 15, 2012 Order, and responded to the recommendations made by the Independent Expert Review Panel. Combined, these two projects identified 273 requirements to assess and 46 percent of those were retired.

Over 50 individuals from industry participated in the SER project this year, which identified over 110 additional requirements to be retired because they were not material to the reliability of the bulk power system. NERC posted the initial Standard Authorization Request (SAR) for industry comment from June 7 through July 10, 2018. The final SAR is posted, and comments are being accepted through September 26, 2018. NERC sought nominations for the Standards Efficiency Review drafting team members being formed to address the recommendations. At this point, Phase 1 of the SER process is complete.

Phase 2 of the process will consider modification, rather than retirement, of Operating and Planning Standards to remove administrative burdens and achieve additional efficiencies.

Achieving Alignment of Standards Implementation through HEROS

Many of you have taken advantage of MRO’s HEROS@mro.net email address to ask questions concerning implementation of the CIP and O&P Standards. So far in 2018, MRO provided 65 responses to registered entities regarding the application of specific requirements.

HEROS@mro.net is your best resource for non-urgent questions related to the application of standards; we strive to answer all questions within 30 days of receipt. If your question requires a more tailored response, we will reach out to you for additional details or to schedule a live conversation. We welcome all questions concerning the application of the Standards and distinguish those from specific implementation questions asking is this “compliant.” An example of a compliance question is: “Our physical security policy does not allow for individuals to make duplicate keys, are we compliant with CIP-006-6?” Whereas, “We are a small entity with only two low impact substations, would MRO be available for a discussion on our proposed approach to physical monitoring and control of those sites without the use of an automated PACS?” is an example of a question related to how to apply a Standard. In that case or the case of a possible noncompliance, send questions to the MRO Risk Assessment and Mitigation Department, who will determine if a self-report is merited.

To read NERC’s most recent Weekly Standards Bulletin, click HERE.

NERC Board of Trustees Adopts Three Reliability Standards; GMD Request Approved

During its recent quarterly meeting in August, the NERC Board of Trustees adopted three Reliability Standards and a GMD data request was approved:

- **BAL-002-3 – Disturbance Control.** The modification to this standard — in response to FERC Order 835 — requires contingency reserve for recovery from a balancing contingency event.
- **CIP-012-1 – Cyber Security, Communications between Control Centers.** This standard requires the protection of sensitive Bulk Electric System data communicated between Control Centers.
- **VAR-001-5 – Voltage and Reactive Control.** The modification to this standard is a result of periodic review and eliminates a duplicative variance requirement.
- **The GMD Data Request** requires transmission and generation owners to provide NERC with their geomagnetic monitoring data to support ongoing research and analysis of GMD risks to the bulk power system. The technical specifications for the data were developed by the Geomagnetic Disturbance Task Force and align with existing industry GMD data capabilities.
SELF-LOGGING
New Self-Log Template Published

Jackson Evans, Enforcement Attorney

MRO is pleased to announce that it has updated its Self-Log Template. The goal of the update is to reduce processing times related to self-logged instances of noncompliance. One of the main motivations behind updating the template was to assist program participants in providing the necessary data so MRO can process the noncompliance without the need for a time-consuming Request for Information (RFI). To process a Compliance Exception, MRO requires specific data points. Dates are one example of these necessary data points (e.g., start date of noncompliance, end date of noncompliance, date of actual or expected completion of mitigating activities) that can be easy for an entity to overlook. MRO found that when using the prior version of the template, program participants would provide significant information regarding the noncompliance and the risk, but would miss one of the numerous dates that MRO is required to provide in a filing. The new template should help registered entities remember this information by providing additional columns that request these required data points.

The updated template was developed with the assistance of our program participants, and MRO extends its thanks to them as well as the MRO Compliance Committee and NERC staff, who also provided comments and feedback during this process. MRO will continue to monitor the effectiveness of the template changes and will continue to make any modifications that will make self-logging more efficient. MRO is committed to improving the Self-Logging Program and streamlining the processing of minimal risk noncompliance. MRO and its registered entities have displayed a strong dedication to the Self-Logging Program. The MRO Region currently has 19 registered entities participating in the Self-Logging Program. Additionally, MRO has recently added Manitoba Hydro, the ERO’s first Canadian program participant, and Southwest Power Administration, the ERO’s first federal entity program participant.

If your organization is interested in the Self-Logging Program, you can contact me directly at jackson.evans@mro.net or mro-self-logging@mro.net.

ELECTRONIC ACCESS POINT
Interface vs. Device

Carl Epping, Risk Assessment and Mitigation Engineer

What is an Electronic Access Point (EAP)?

During MRO’s compliance monitoring and outreach programs, MRO discovered that there is confusion among some entities regarding Electronic Access Points (EAP). In conjunction with the CIP version 5 standards, NERC defined an Electronic Access Point as “A Cyber Asset interface on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.” The key word in the definition is interface – this explicitly refers to the interface, or port, on a device and not the device itself. This is a departure from the CIP version 3 standards (CIP-005-3a), where the EAP was not defined, but instead was considered to be the device (e.g. firewall).

Why does interface vs. device matter?

By identifying the interface as an EAP rather than
the device, the standard allows for more flexibility in applying the rules surrounding the EAP. One example of this may be at a substation (see Figure 1), where a switch is used for corporate Cyber Assets as well as medium or high impact BES Cyber Assets (BCA). The port or ports used for the BCAs are now identified as an EAP(s), limiting the Electronic Security Perimeter (ESP) to those BCAs. Under CIP version 3, a separate device was needed to act as the EAP, or all the Cyber Assets would have been included in the ESP.

Additionally, by identifying the EAP as an interface, scrutiny of firewall rules is limited to that interface, simplifying compliance. For example, in a situation where there is a DMZ outside the ESP, an external corporate interface, and a single EAP for a BES Cyber System, only the latter would be in scope under CIP-005-5 R1.1 (see Figure 2).

What else should be considered?

CIP-005-5 R1.1. Consideration should be taken when identifying EAP(s) on a device due to this requirement. As a simple example, for a firewall with one interface connected to a BCS and one interface connected to the outside world, the EAP can be defined as either interface. Note, however, that identifying the outside interface of the firewall as the EAP now places the firewall itself inside the ESP, which then makes it a Protected Cyber Asset (PCA) in addition to already being an Electronic Access Control or Monitoring System (EACMS). As a PCA, it is now in scope for all PCA requirements, in particular the requirement for the use of an Intermediate System for Interactive Remote Access.

CIP-005-5 R1.2. The requirement states that “All External Routable Connectivity must be through an identified Electronic Access Point (EAP).” There are a number of ways EAPs can be identified, but they must be identified. Some entities use spreadsheets, policies, diagrams, or a combination thereof. Many entities have found the identification on network diagrams to be the most beneficial as it helps in clearly delineating where the ESP is in relation to the EAP and also helps with compliance activities.

CIP-005-5 R1.3 – Both inbound and outbound rules must be applied at the EAP interface. Having only ingress rules applied to each interface on a firewall is no longer sufficient, since both ingress and egress rules must be applied at the EAP. As mentioned above, this actually helps with compliance as only the rules on identified EAPs are in scope.

Questions regarding Electronic Access Points can be directed to HEROS@midwestreliability.org.
Industry Tips and Lessons Learned

CIP-002 SELF-CERTIFICATION
Impacts From Risk-Based Oversight

Jess Syring, CIP Compliance Engineer

As many of you are aware, the CIP-002 self-certification will be issued on October 1, 2018. Many entities are planning to receive this self-certification based on their current Compliance Oversight Plan (COP). MRO has decided to modify the distribution of the CIP-002 self-certification as part of our efforts to further implement risk-based oversight. MRO has taken into consideration each entity’s inherent risk, results from past Compliance Monitoring Enforcement Program (CMEP) activities, mitigation history, and known internal controls.

This will most affect those entities that have been in the MRO region for a longer time-period because of their aggregated compliance history. Entities that have demonstrated high-performing capabilities for CIP-002 to MRO will not receive this self-certification.

At this time, MRO does not intend to issue revised COPs to reflect these changes. If your entity does not receive the self-certification on October 1, 2018, your entity is not subject to respond. If you have any questions on this change, please contact Jess Syring at jess.syring@mro.net.

MRO ACQUIRES NEW DOMAIN NAME
Tips For Ensuring Message Delivery

Alex Pratt, Manager of IT Infrastructure

MRO recently made changes to its website and email structure, changing the primary domain and website from midwestreliability.org to mro.net. Email formats were also changed to a first-name.lastname format. Since then, it’s come to our attention that emails going out from MRO have not been reaching some folks, especially when names are part of contact lists.

To ensure email messages are received and delivered as intended, please:

- Check email lists to make sure MRO emails have been properly updated with new email addresses.
- Check spam filters to verify that all email addresses with domain mro.net and midwestreliability.org are allowed.
- Check all mailbox rules to allow *@mro.net addresses.
- Work with your IT staff to ensure any corporate-wide protection systems are allowing and white-listing *@mro.net email address and domains.

If you have any questions, or feel that you haven’t been receiving email messages from MRO, please reach out to MRO IT so any issues can be resolved.

NERC Lessons Learned

NERC’s Resource Center makes educational products available to Regional Entities, industry participants, and regulators.

NERC also publishes documents to convey lessons learned from NERC’s various activities. New lessons learned from August are:

- Firewall Failure After Time Limit Exceeded
- Loss of Substation Data Circuits to SCADA

Follow the below links for Tips, Lessons Learned and Publications in other Regions:

- Florida Reliability Coordinating Council (FRCC)
- SERC Reliability Corporation (SERC)
- Texas Reliability Entity (Texas RE)
- ReliabilityFirst (RF)
- Western Electricity Coordinating Council (WECC)
- Northeast Power Coordinating Council (NPCC)
CONFERENCE OVERVIEW

Midwest Reliability Organization (MRO) is pleased to announce it is hosting a Fall Reliability Conference at its offices in Saint Paul, Minnesota and via a live WebEx stream. This one-day conference will focus on topics related to integration of renewables and related transmission expansion.

PRELIMINARY AGENDA TOPICS

- Transmission Expansion to Integrate Renewables
- Power from the Prairie
- SOO Green Renewable Energy Delivery Project
- Changing Load Characteristics
- Inertia 101
- Great Northern Transmission Line Project
- Challenges of Integrating Large Scale Renewable Generation
- Wind from the Dakotas and Pumped Storage
- Hawaii Energy – Integration of Renewables

REGISTRATION

Technical staff, subject matter experts, and power system engineers from entities are encouraged to attend this free conference. You may register to attend in-person or by WebEx here.

LODGING

MRO has a room block at the Hampton Inn & Suites at $169/night. The deadline for this reduced rate is September 22, 2018, or until full. Click here to make your reservation or call 651-224-7400. For other hotels in the downtown Saint Paul area, please see MRO’s visitor packet.

For questions regarding this conference, please contact Lisa Stellmaker. For registration, travel or lodging assistance, please contact Chris Adam, Administrative Meeting Coordinator, at 651-855-1743.
This CMEP Summary Report is the first in a series of transitional editions to integrate data from the former SPP RE registered entities into the existing metrics. This report focuses on enforcement metrics; risk metrics will be added as analytics are completed. Additional explanations are included as needed for each metric to clarify how data from these new MRO entities has been integrated. These explanations will continue to be included in the transitional editions and, if desired, beyond. Our objective, as always, is to include metrics and information that provide value, and we welcome your feedback on these reports.

Compliance Update

Compliance Oversight Plans (COP)

The MRO Compliance Department is developing multi-year COPs for all registered entities. All BA, RC, and TOP entities, registered with MRO as of January 1, 2018, have received COPs. As reported in previous months, MRO was going to begin sending draft multi-year COPs for the non-BA, RC, TOP registered entities (registered with MRO as of January 1, 2018) to the entities for comment; however, given the current ERO collaboration project on COPs, MRO has postponed sending the draft COPs to non-BA, RC, and TOP registered entities. The schedule for issuing the COPs for transitioning SPP RE entities is being developed in tandem with the IRA refresh process.

2018 Compliance Audit Status

MRO has completed six of thirteen audits scheduled in 2018. Additionally, MRO provided resources to assist SPP RE with three audits and NERC with one audit. Please visit MRO’s website to view MRO’s 2018 audit schedule and the draft 2019 audit schedule.

2018 Self-Certifications

Registered entities have started to respond to the 2018 Q3 self-certifications for MOD-026-1 R2, MOD-027-1 R2, MOD-032-2 R1, R2, R3, R4, and CIP-008-5 R1, R2, R3. MRO’s goal is to have all Q3 self-certifications reviewed by the end of Q4 2018.

Risk Assessment and Mitigation Update

HEROs Update

The MRO Risk Assessment and Mitigation (RAM) Department continues to answer questions from registered entities and provide HEROs information to entities that transitioned into MRO as a result of the SPP-RE dissolution. MRO staff continues to closely follow the CIP V5 revisions, CIP-012 (Communications between Control Centers), and work being done to clarify SOLs and IROLs. MRO continues to encourage registered entities to submit technical questions via email to MRO at: HEROS@mro.net

Transfer of SPP RE Open Noncompliances

As of July 1, 2018, 90 open noncompliances from the SPP RE region have been transferred into MRO, which is approximately a 44% increase in cases. MRO RAM staff has been in contact with each of the former SPP RE entities with open noncompliances to discuss risk and mitigation of the noncompliances.

Risk Determinations Associated with Self-Logged Noncompliances

There are currently 19 entities participating in the Self-Logging program. All instances of noncompliance self-logged by registered entities that have been processed have been resolved as Compliance Exceptions.

Additional Metrics to Follow

The risk and mitigation metrics and statistics are being updated to include the newly registered entities’ data in order to provide a holistic metric for the region and will be included in future reports. Risk Determinations

Enforcement Update

Revisions to Hearing Procedures

On June 8, 2018, FERC issued a letter order approving changes to the NERC Rules of Procedure that incorporate the Consolidated Hearing Process, which...
provides a uniform and more streamlined approach to hearings. The MRO GPC will provide its recommendation for the adoption and integration of this process to the MRO Board of Directors at the October MRO Board Meeting.

**Noncompliance Trends and Statistics**

The charts at right reflect a breakdown of all CIP vs. Non-CIP Possible Instances of Noncompliance by Year Discovered and Reported to NERC as of August 31, 2018.

In the following Noncompliance Statistics and Noncompliance Trends charts, the numbers reflect all noncompliances in the MRO region which are defined as 1) all the MRO noncompliances, both open and closed, that were reported to NERC as of August 31, 2018, and 2) all of the open noncompliances that were transferred to MRO from SPP RE on July 1, 2018. These charts plot this group of noncompliances by the year in which they were discovered.

**Noncompliance Trends and Statistics**

**Registered Entity Responsibility**

MRO staff trends how often registered entities self-identify and accept responsibility for noncompliance. These metrics are an indicator of the commitment to overall governance for compliance among registered entities in the region. The high percentages for both metrics demonstrates a strong governance and compliance culture in the MRO region, as well as registered entities’ willingness to accept, and learn from, discovered noncompliances in order to prevent future noncompliance.

(Continued on page 20)
As with the preceding metrics, the numbers for each year in the chart at right include noncompliances for entities that were registered in the MRO region during that year. Therefore, noncompliances for entities from the SPP RE region that were registered in the MRO region on July 1, 2018, are included in the 2018 numbers.

The pie charts at right show the percentage of time that registered entities have accepted responsibility for noncompliances filed with NERC. The noncompliances for the entities from the SPP RE region that were registered in the MRO region on July 1, 2018, are included in the 2018 numbers, and are included in both charts.

**Discovery Method Detail (June 18, 2007 through August 31, 2018)**

In the Discovery Method chart on page 21, the numbers reflect all noncompliances in the MRO region that are defined as 1) all the MRO noncompliances, both open and closed, that were reported to NERC as of August 31, 2018, and 2) all of the open noncompliances that were transferred to MRO from SPP RE on July 1, 2018. This chart plots the noncompliances by the year in which they were discovered.

**Noncompliance Processing**

As with the previous metrics, the pie charts on page 21 include noncompliances for entities that were registered in the MRO region during the specified time frame. Therefore, noncompliances for the entities from the SPP RE region that were registered in the MRO region on July 1, 2018, are included in the 2018 numbers, and are included in both charts.
Compliance Exceptions

As with the previous metrics, the Compliance Exceptions Processed metric and narrative below include noncompliances for entities that were registered in the MRO region during that year. Therefore, these entities’ noncompliances are included in both of the column charts on page 22, as well as the following narrative, as they include 2018 noncompliances.

MRO processed 270 findings as CEs from July 1, 2014, the date on which CEs became eligible for filing, to August 31, 2018, (167 CIP and 103 Ops and Planning); of the 270 CEs, 210 were Self-Identified. For 2018, MRO processed 86 CEs (63 CIP and 23 Ops and Planning); of the 86 CEs, 79 were Self-Identified.

Status of Alleged and Confirmed Instances of Non-Compliance

As with the previous metrics, the table on page 22 includes noncompliances for entities that were registered in the MRO region since 2007 and noncompliances for the entities from the SPP RE region that were registered in the MRO region as of July 1, 2018.

For questions on this CMEP report:

Compliance Department: compliance@mro.net
Risk Assessment & Mitigation Department: HEROS@mro.net
Enforcement Department: enforcement@mro.net

(Continued on page 22)
Compliance Exceptions

Compliance Exceptions Processed (July 1, 2014 - August 31, 2018)

- CIP Standards
  - Self-Identified: 137
  - Region Identified: 30

- Operations & Planning Standards
  - Self-Identified: 73
  - Region Identified: 30

Status of Alleged /Confirmed Instances of Noncompliance

Compliance Exceptions Processed (January 1, 2018 - August 31, 2018)

- CIP Standards
  - Self-Identified: 61
  - Region Identified: 2

- Operations & Planning Standards
  - Self-Identified: 18
  - Region Identified: 5

Status of Possible Noncompliance & Confirmed Violation Process (Backlog)

<table>
<thead>
<tr>
<th>Findings Category</th>
<th>Total</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Number of Findings</td>
<td>1357</td>
<td>100%</td>
</tr>
<tr>
<td>Number of Dismissals</td>
<td>278</td>
<td>20%</td>
</tr>
<tr>
<td>Number of Findings Processed</td>
<td>847</td>
<td>62%</td>
</tr>
<tr>
<td>Number of Findings Awaiting Filing or Posting</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>Number of Findings Outstanding</td>
<td>232</td>
<td>18%</td>
</tr>
</tbody>
</table>

ERO Enterprise-Endorsed CMEP Implementation Guidance

A key factor in the success of compliance monitoring and enforcement of mandatory standards rests on a common understanding among industry and ERO Enterprise CMEP staff of how compliance can be achieved and demonstrated. For many standards, this is straightforward. For others, a variety of approaches may achieve the same objective.

Implementation Guidance is developed by industry and vetted through pre-qualified organizations. Vetted examples can then be submitted to the ERO Enterprise for endorsement, and, if endorsed, the ERO Enterprise would give the example deference during CMEP activities with consideration of facts and circumstances. Implementation Guidance would not prescribe the only approach to implementing a standard and entities may choose alternative approaches that better fit their situation.

ERO Enterprise-endorsed Implementation Guidance can be found on [NERC’s website](http://www.nerc.com).

Questions about compliance guidance should be directed to [complianceguidance@nerc.net](mailto:complianceguidance@nerc.net).
NATIONAL/INTERNATIONAL NEWS

NERC's Sena Named to Task Force to Explore Puerto Rico Energy Solutions
September 11, 2018—Janet Sena, Senior Vice President and Director of Policy and External Affairs at the North American Electric Reliability Corporation, was appointed to the Southern States Energy Board (SSEB) Blue Ribbon Task Force. Read more.

FERC to Convene Technical Conference
September 10, 2018—The Federal Energy Regulatory Commission (FERC) has announced it will hold a technical conference, after the October 2018 Commission public meeting, to hear from the Regional Transmission Organizations (RTOs) and Independent System Operators (ISOs) on their efforts for ensuring reliable and economic system performance during the 2018-2019 winter season. Read more.

FERC Approves Revised MRO Bylaws
September 6, 2018—On September 6, 2018, the Federal Energy Regulatory Commission (FERC) approved the revised MRO Bylaws that were submitted by the North American Electric Reliability Corporation (NERC) on June 4, 2018. Read more. Read the FERC Order.

Karen S. Evans Sworn in as First DOE Assistant Secretary for Cybersecurity, Energy Security and Emergency Response
August 28, 2018—Karen S. Evans was confirmed by the U.S. Senate and sworn in by U.S. Deputy Secretary of Energy Dan Brouillette as the Assistant Secretary for the Office of Cybersecurity, Energy Security, and Emergency Response (CESER). Read more.

Bill Lawrence Named NERC Vice President and Chief Security Officer
August 7, 2018—NERC's Board of Trustees named Bill Lawrence as vice president and chief security officer, effective August 16. Read more.

REGIONAL NEWS

MN PUC Commissioner Appointed to NARUC Board of Directors
September 11, 2018—The National Association of Regulatory Utility Commissioners (NARUC) has appointed Dallas Winslow, the chairman of the Delaware Public Service Commission, and Matthew Schuerger, a commissioner on the Minnesota Public Utilities Commission, to its board of directors. Read more.

Kansas Top Wind Producer According to DOE Report
August 26, 2018—Kansas is a top producer of wind-generated energy, a U.S. Department of Energy study found, confirming what leaders at Westar Energy have known for years. Read more.

INDUSTRY EVENTS

Please Note: Any of the events listed below are some of many training opportunities that may be of interest to MRO Members and other readers of the MRO newsletter. MRO neither recommends nor endorses any particular vendor or event.

MRO to Host 2018 Annual Security Conference
September 26, 2018—MRO will host its 2018 Annual Security Conference preceded by a day of technical training at its offices in Saint Paul, MN. More information on the conference and agenda are available here.

NERC to Host Monitoring and Situational Awareness Technical Conference
October 2-3, 2018—The North American Electric Reliability Corporation (NERC) will host its sixth annual Monitoring and Situational Awareness Technical Conference on October 2-3, 2018 at MISO in Carmel, Indiana. The theme of this year’s conference is The Evolution of EMS Systems. Register here. Hotel and travel information can be found here.

Registration Now Open for GridSecCon 2018
October 16-19, 2018—NERC’s Electricity Information Sharing and Analysis Center and the Western Electricity Coordinating Council are hosting the eighth annual grid security conference on October 16-19 in Las Vegas. Read more here.

MRO to Host Fall Reliability Conference
October 24, 2018—MRO will host its Fall Reliability Conference at its offices in Saint Paul, MN. Registration will be available soon here.

MRO to Host 2018 Annual CMEP Conference
November 14, 2018—MRO will host its Annual CMEP Conference at its offices in Saint Paul, MN. Registration will be available soon here.

If you have regional news or events you’d like to report, please contact Jessie Mitchell.
CONTACT LIST

Main Phone: 651-855-1760
Main Fax: 651-855-1712
Web: www.mro.net

General & Executive
Sara Patrick, President and CEO (1708)
Richard Burt, Sr. VP and Chief Operating Officer (1714)
Miggie Cramblit, VP General Counsel, Corporate Secretary and Director External Affairs (1721)
Jessica Mitchell, Stakeholder Outreach and Communications Principal, Assistant Corporate Secretary (1733)
Carolina Margaria, Administrative Assistant (1739)

Finance and Administration
Sue Clarke, VP Finance & Administration (1707)

Enforcement
Val Agnew, VP Enforcement (1745)
Janice Anderson, Enforcement Paralegal (1720)

Compliance
Jeff Norman, Director of Compliance Monitoring (1703)
Desirée Sawyer, Compliance Monitoring Coordinator (1730)

Mitigation and Standards
Bill Steiner, Director of Risk Assessment and Mitigation (1718)
Dana Klem, Risk Assessment and Mitigation Administrator (1741)

Operations (Assessments, Event Analysis)
Dan Schoenecker, VP Operations (1753)
Lisa Stellmaker, Operations Administrator (1749)

After Hours Emergency Line
651-734-8355

To report an MRO Region Event:
events@mro.net

MRO 2018 Calendar of Events:

SEPTEMBER
9/20-21/2018 Closed GPC Meeting
9/25/2018 MRO Technical Training
9/26/2018 MRO Security Conference
9/27/2018 MRO Security Advisory Council Meeting

OCTOBER
10/3/2018 MRO Board Closed Executive Session
10/4/2018 MRO Board of Directors Meeting
10/17/2018 MRO Compliance Committee Webex
10/18/2018 MRO Standards Committee Webex
10/23/2018 MRO Planning Committee Meeting
10/24/2018 MRO Fall Reliability Conference
10/25/2018 MRO Operating Committee Meeting
10/30/2018 Closed GPC Committee Meeting

NOVEMBER
11/1/2018 Fourth Quarter FAC Meeting
11/8/2018 MRO Security Advisory Council Meeting
11/14/2018 MRO CMEP Conference
11/28/2018 Closed GPC Meeting In Person Meeting
11/28/2018 MRO BOD Closed Executive Session
11/29/2018 MRO Annual Member and Board Meeting

REMAINING MRO OFFICE CLOSURES
11/22/2018 Thanksgiving
11/23/2018 Thanksgiving
12/24/2018 Winter Holiday
12/25/2018 Winter Holiday

A complete list of events can be found on MRO’s website calendar.