Inside This Issue:

Industry Matters
- Adaptive Cybersecurity Regulation (Page 2)
- From the Board Chair (Page 4)
- It's All About Reliability (Page 6)
- Industry News and Events (Page 26)

Regulatory Affairs and Enforcement
- International Oversight of the Regional Bulk Power System (Page 5)

Bulk Power System Security
- GridSecCon 2017 (Page 11)
- Responding to SCADA Malware May Require Stepping Up Our Game (Page 12)
- Security Corner (Page 14)
- MRO to Host 2017 Security Conference (Page 15)

Bulk Power System Operations
- Joint Study on Bulk Power System Restoration and Recovery (Page 16)

Reliability Standards and Registration
- NERC Standards Update (Page 9)
- NERC Webinar on Geomagnetic Disturbance Mitigation (Page 9)

Compliance Monitoring and Enforcement Program
- CMEP Report and Dashboard (Page 22)

Tips and Lessons Learned
- Compliance Oversight Plans: Taking Risk-Based Compliance Monitoring to the Next Level (Page 18)

Elevating Ethics
- The Cost of Inaction (Page 20)

Finance and Administration
- Year-to-Date Financials; 2018 Business Plan and Budget Process and Timing; Culture and Talent Management (Page 19)
- Employee News and Meeting Calendar (Page 27)

MRO Reads
- Dave’s Subs: A Novel Story About Workplace Accountability (Page 10)

Share your feedback!
Please let us know what information is important to you. To submit story ideas or other suggestions for Midwest Reliability Matters, please contact Jessie Mitchell at 651-855-1733
Cybersecurity represents one of the greatest challenges facing our industry today. Since the cybersecurity Reliability Standards became mandatory with the initial Critical Infrastructure Protection (CIP) Version 1 in 2008 and Versions 2-3 effective in 2010, the Standards have remained in a state of flux—a constant churning of new and improved versions to address the unrelenting advancement of threats. And while the Standards churn on, the cyber-attacks have intensified. The latest, a malware attack called “CrashOverride,” specifically targeted our industry. This is possibly the first time North America will face a Stuxnet-type threat.

One of the key challenges in developing Standards to address cyber risk is balancing the various existing technical configurations and emerging technologies with language that can accommodate both. Another challenge is assuring the Standards do not result in homogeneous solutions across the interconnected system. Our current system diversity is a formidable defense against catastrophic failures. Drafting uniform requirements that still maintain this diversity is a daunting task for standards developers.

Therefore, addressing cyber risk is an extremely complex task. Nevertheless, in the face of complexity, we should not add more complexity. By doing so, we actually make things worse—like pouring gasoline on a fire. Adding complexity through more prescriptive regulation shifts the focus towards compliance, rather than security. Security and compliance are not necessarily the same. If Standards were perfectly designed around security, then compliance would simply be a byproduct of security. However, we’ve learned that the pursuit of perfection in the cybersecurity Standards does not have a good payback—it creates churn. By the time a new threat or emerging technology is addressed in the Standards, something newer, and more advanced has come along. An unintended consequence of the current CIP Standards is planned obsolescence. This churning of the Standards creates uncertainty, which introduces risk and increases costs.

So how do we effectively and efficiently protect the bulk power system in this incredibly complex cyber environment?

We respond to perpetual, complex change through adaptation. As Darwin once said, “it’s not the strongest or the smartest who survive, but those who adapt.” That should be our cybersecurity motto. Instead of perfecting the Standards as a primary line of defense, maybe we should look at changing how we monitor compliance and enforce the Standards (we cannot depend on a Maginot line as a line of defense because it can be outflanked). But, we can acknowledge that Standards for cybersecurity will never be perfect and outflanking will be a common threat vector. As we all know, Standards cannot keep up with the emerging threats or new technologies—the speed of change eclipses the protection of the Standard. There will always be situations where compliance may be suboptimal for cybersecurity—and, entities should be encouraged to reach for higher cybersecurity without the specter of irrational regulatory responses that result in reduced cybersecurity to meet dated compliance requirements.

Being adaptive requires thinking about alternatives and here are some of my alternatives to reconcile compliance with cybersecurity.

One alternative, which I’m calling the “reverse TFE,” addresses situations where a registered entity has deployed superior cybersecurity, but does not meet compliance with a Standard.
these situations, MRO should be able to deem the entity compliant because it has reasonably demonstrated that the technical configuration, approach, process, etc., meets or exceeds the intent or purpose of the Standard. This result in a sort of “reverse TFE” or a waiver from strict compliance with specific CIP requirements as long as the configuration, approach, etc., is implemented as designed in the waiver. This will also help us move entities from having two sets of books—one for cybersecurity and one for compliance. In turn, these waivers could be used as feedback loops to improve the Standards process and inform entities, similar to OODA.⁴

A second alternative would be to recognize that some, mostly larger system owners and operators, have already adopted cybersecurity frameworks, which encompass and/or overlap CIP, such as ISO,² ITIL,⁶ COBIT,⁷ NIST,⁸ etc. In these situations, perhaps MRO staff should assess cybersecurity based upon the framework being used by the entity as applied to its SCADA/EMS and related Bulk Electric System facilities. At the end of the assessment, the entity can either agree with mitigation for potential performance gaps against the framework or disagree with the performance gap. If there were a disagreement, MRO staff would map the gap to a CIP requirement for due process as a potential violation. If there are no requirements to map, the performance gap would be either a recommendation or an area of concern, depending on the risk. Given MRO has broad discretion in enforcement, why not leverage broad, technical judgment in determining whether the purpose of the Standard has been met?

As a third alternative, instead of “requirement-based” standards, which are more specific, we could change to “objective-based” standards, which are less specific. For example, we could translate the NIST and CIP frameworks to cybersecurity objectives. Under this alternative, Reliability Standard CIP-007 Security System Management could be translated to the Security Objective—Prevent Malicious and/or Unauthorized Code on Control Systems. Just to be clear, “objective-based” standards are not “results-based” standards or “performance-based” standards. Both of these types of standards are backward looking, not forward looking. Cybersecurity objectives and our evaluations are to be forward looking. MRO would then measure compliance to the security objective by asking, “can you show me how you meet this cybersecurity objective?” MRO staff would document how the entity meets the cybersecurity objective and if we have findings or deficiencies, they would have similar dispositions as today. Like the other alternatives, there is more latitude in applying the intent or objective of the Standard, rather than “checking the box” for the requirements—more like the former Readiness Audits or current Certifications. This is the most elegant approach because it is all about the cybersecurity objectives—we do not get lost in a sea of adminstrivia around requirements and sub-requirements. What a delightful change in the conversation between the regulator and the regulated.

Although none of the alternatives I’ve laid out here are easy or perfect, they allow for a more sustainable approach to addressing cyber risk. We can start small—MRO could pilot an alternative with a couple of registered entities, report back to NERC and FERC.

The goal is to improve cybersecurity—we can improve cybersecurity by adopting approaches that encourage more dialogue, improve problem solving, and encourage creativity to secure our systems. We need a better approach. Is change risky? Yes. Is it worth it? Yes. As Frederick Douglass once said, “If there is no struggle, there is no progress.”

---

⁴ Observe, Orient, Decide, Act—decision cycle developed by U.S. Air Force, which emphasizes agility over power.
⁵ International Standards Organization
⁶ Information Technology Infrastructure Library
⁷ Control Objectives for Information and Related Technologies
⁸ National Institute of Standards and Technology
FROM THE MRO BOARD CHAIR

Dear Members and Stakeholders:

Last month NERC’s Critical Infrastructure Protection Committee (“CIPC”) held its second Technologies Roundtable where the issues of cloud services and the CIP standards were discussed by NERC staff, industry experts, and technology and cybersecurity experts. Cloud services have been and will continue to be a hot topic for the ERO, the Critical Infrastructure Protection Committee, and industry for some time.

Synchrophasors, relays, transformers, and switches on the Bulk Electric System (“BES”) and connected to control centers are creating increasingly vast amounts of data each day. To maximize the value of this data, storage and access, together with security and compliance, must occur at a reasonable cost. Transmitting and storing data in the cloud would allow registered entities to realize the full value of the data. The question the ERO and industry must address is: Can we secure that operational data and those critical systems from evolving cyber threats if we use cloud services and other emerging technologies?

Whether the industry can securely leverage the cloud and other technological advancements will impact the future of security and reliability of the BES. MRO has made BES physical and cybersecurity and availability of operating systems a key focus and will continue to stay abreast of the efforts expended by FERC, the ERO, and the industry on the ever-evolving CIP standards and what can be done to stay ahead of cybersecurity intrusions without adding additional CIP administrative compliance obligations that do not enhance security. As we have said in the past, compliance may not necessarily equal security.

So how do we use these technological advancements while at the same time ensure the security and availability of systems on which we are so dependent? One thing that we do know is that continuing revision of and development of new CIP standards may not be the best or the only answer. We must be mindful of how we use expert cyber and security resources so that we aren’t diverting and diluting their cyber data mining and intrusion defense efforts to revision and development of CIP standards, particularly if implementation of those standards does not increase security, but merely increases, as Dan Skaar likes to say “administrivia.”

Some of the CIP standards are on their sixth or seventh revision in eight years of mandatory compliance. This level of change creates administrative work that does not improve the security or reliability of the BES. Both industry and the ERO created this history and together we can do better. The ERO is focusing on higher risk security issues; this encourages the proper use of security resources and should reduce compliance costs as the risk-based compliance framework moves forward. This shift also encourages industry to lead the development and design of the “what” of CIP standards or security frameworks and move away from “how” to comply standards and their inherent administrative burden. Continuing down this path will allow the registered entities to focus on security first with compliance becoming a natural outcome of good security practices.

In this context, we can begin to consider whether cloud services provide meaningful enhancements to security and the reliability of the BES? My short answer to this inquiry is yes. A few cloud services providers have published white papers suggesting that their cloud services enhance a registered entity’s security and comply with the CIP standards. Information on the Technologies Roundtable and cloud services can be found on the NERC website here. In fact, one cloud service provider has announced that it has mapped every CIP standard and requirement to its cloud service controls and believes its systems to be compliant with the CIP standards. NERC has stepped up its efforts to work with cloud service providers to assess their security efforts and determine how compliance could work and be monitored by the ERO.

(Continued on page 5)
There are fundamental security questions that we need to address under existing standards to ensure security of operational data before moving this data to the cloud. How will the ERO audit the physical and cybersecurity of these cloud servers? One cloud service provider indicates that only servers located in certain areas in the U.S. will be used for CIP confidential information and some cloud service providers believe that certain CIP standard definitions will need to be modified in order to utilize their cloud service options.

Will the benefits of cloud services outweigh the effort and cost to use the cloud? I think so. Industry must continue to embrace available technological enhancements, including cloud services, which offer new tools to get ahead of evolving security and reliability threats but not at the price of security. I am optimistic that the ERO and the industry will get to the right solution when it comes to the relationship between using new technologies, including cloud services, and the CIP standards, but it won’t happen tomorrow. I am also encouraged that we at MRO are actively participating in the cloud services discussions and continue to push for technological answers to improve security and reliability.

(Continued from page 4-From the MRO Board Chair)

Sara Patrick, VP Compliance Monitoring and Regulatory Affairs

As a cross-border Regional Entity, MRO operates under unique regulatory constructs and agreements with the provinces of Manitoba and Saskatchewan for compliance and enforcement of Reliability Standards. Below is summary of MRO’s regulatory activities in Manitoba and Saskatchewan.

Manitoba

On April 21, 2017, an updated list of Reliability Standards, which includes the CIP Version 5 Standards, was adopted in the province and became effective on July 1, 2017. As it worked through the updates of NERC Reliability Standards, the Manitoba Government shared some concerns with MRO staff related to NERC Reliability Standard TPL-001-4 and the requirement to implement Corrective Action Plans, which include “installation, modification, retirement, or removal of Transmission and generation Facilities and any associated equipment” (TPL-001-4 R2.7.1). According to The Manitoba Hydro Act, a Reliability Standard may not “have the effect of requiring the construction or enhancement of facilities in Manitoba.” (Manitoba Hydro Act 15.01(2).) The updated list of Reliability Standards does not include TPL-001-4. Instead, Manitoba Hydro has approved the adoption of a similar Manitoba Hydro Reliability Standard, MH-TPL-001-4, adopted under the provisions of The Manitoba Hydro Act. MH-TPL-001-4 requires obtaining “all applicable corporate, regulatory, provincial, and federal evaluations and approvals” prior to implementing a Corrective Action Plan. MH-TPL-001-4 also took effect on July 1, 2017, when the updated list of Reliability Standards from the Manitoba Government became effective. MRO is working with Manitoba Hydro on developing an MOU to conduct compliance monitoring of MH-TPL-004-1 and possibly other Manitoba Hydro Reliability Standards that may be adopted in the future.

Saskatchewan

In October 2016, the Saskatchewan Electric Reliability Authority (SERA) adopted the NERC Rules of Procedure related to Entity Registration, Compliance Monitoring and Enforcement, and Standards Adoption in the province. Under the Entity Registration procedures, MRO staff worked with SERA to evaluate entities and determine whether they should be registered and subject to mandatory compliance with NERC Reliability Standards. On February 1, 2017, three entities were registered with NERC and will be subject to mandatory compliance with NERC Reliability Standards. On February 1, 2017, three entities were registered with NERC and will be subject to mandatory compliance monitoring and enforcement in Saskatchewan. The newly registered entities have 18 months to become compliant with the applicable NERC Reliability Standards. It is anticipated that additional entities will be registered in the province, but the timing is uncertain as staffing changes resulted in the loss of a quorum for SERA, which has since been restored.
June 18, 2007, is a significant date for our industry. It is the date compliance with NERC Reliability Standards became mandatory and enforceable. Over the past decade, there has been significant change in MRO’s Compliance Monitoring and Enforcement Program (CMEP) approach, yet through it all one theme runs strong—it’s all about reliability.

The MRO Board of Directors crafted the MRO Vision: *Maintain and improve the quality of life through a highly reliable regional Bulk Power System.* To achieve this vision, MRO staff focuses on the MRO Purpose: *Strive to assure each Bulk Power System owner and operator within our region is a Highly Effective Reliability Organization (or HE-RO).* Toward that end, we are accountable for results, we provide clarity and assurance of procedures, processes, and controls to improve the reliability of the bulk power system. We deliver meaningful outcomes to those we serve and use our funding wisely. We embrace our public trust obligation to be independent and transparent. We are collaborative in approach and seek constructive solutions.

As we look back at the last decade, it is clear that MRO’s approach to executing its CMEP responsibilities has evolved, improved, and matured, hand in hand with our registered entities’ efforts to not only maintain compliance with NERC Reliability Standards, but also to achieve reliability excellence.

### 2007-2008

In the initial days of mandatory compliance, an annual Actively Monitored List of Standards and Requirements was published and MRO audited registered entities for compliance with these prescribed Reliability Standards on a predictable three-year or six-year schedule, based on functions for which they were registered. MRO required Mitigation Plans for every Possible Violation, regardless of risk to the reliable operations of the bulk power system. Full Notices of Penalty were filed for every enforcement action, sometimes reaching upwards of 35 pages for two minimal risk violations. While there was an initial six-month period allowing Regional Entities to exercise discretion in enforcement actions, thereafter, penalties were expected to be levied for each violation, and were typically in the $5,000-$15,000 range.

In early 2008, MRO negotiated the first settlement agreement in North America for violations of NERC Reliability Standards. It is important to note that the proposed penalty was offset by the registered entity’s agreement to make investments in tools and training. Even in those early days of mandatory enforcement, MRO recognized the value of investments in lieu of penalties to improve reliability and reduce risk to the bulk power system.

### 2009-2010

As MRO gained experience with its CMEP responsibilities, our processes began to evolve and improve. Our view of risk matured. To better achieve our objectives, MRO adopted a three-step approach to executing its CMEP responsibilities. The three steps include: Compliance Monitoring, which includes conducting compliance audits, spot checks, and self-certifications; Risk Assessment and Mitigation, which includes gathering facts and circumstances to assess actual and potential risk associated with each noncompliance and developing and monitoring mitigation efforts; and Enforcement, which includes pro-
cessing of noncompliance and assessment of any associated penalties or sanctions.

As a precursor to more streamlined enforcement mechanisms, the Administrative Citation Process was introduced and implemented within MRO. During this time period, many enforcement actions were resolved through the settlement process. MRO consistently encouraged registered entities to propose “above and beyond” activities as an offset for proposed penalties.

MRO also began implementing a more comprehensive approach to mitigation that focused on risk to reliability and implementing management practices to detect, prevent, and correct noncompliance. Not only does this approach serve our objective of improving reliability, it also reduces recidivism because the underlying cause is addressed. Concurrent with the comprehensive approach to mitigation, MRO began conducting technical assessments of the risk posed by all noncompliance, utilizing engineers and those with cyber expertise to work with registered entity subject matter experts to gain a shared understanding of risk posed by the noncompliance.

2011-2012

As CMEP processes evolved, it was clear that the focus was changing. No longer was the focus on compliance risk, but instead the focus was on reliability risk. In the enforcement process, MRO formally recognized that the acceptance of responsibility for noncompliance was fundamental to maintaining reliability. Streamlined enforcement mechanisms were implemented, including Find, Fix, Track and Report (otherwise known as FFT) and the Spreadsheet Notice of Penalty, which reflected more appropriate means of resolving lower risk noncompliance.

During this time, the Reliability Assurance Initiative (RAI) was launched across the ERO. The intent of the RAI was to re-engineer the compliance and enforcement approach by: 1) recognizing a registered entity’s risk and its management practices around risk in the scope and conduct of our work; 2) recognizing and rewarding registered entities who design and implement strong preventive, detective and corrective action programs; 3) reserving enforcement proceedings for significant matters by creating a new path for resolving noncompliance outside of enforcement; and 4) reducing administrative compliance burdens across the ERO.

2013-2014

As the RAI was being developed, MRO increased its stakeholder outreach efforts. Standard Application Guides were being developed by Subject Matter Expert Teams under the direction of the MRO Standards Committee. The Performance and Risk Oversight Subcommittee began discussing and developing model internal controls under the direction of the MRO Compliance Committee. The RAI began considering how to incorporate inherent risk considerations and our understanding of individual entity management practices into compliance oversight, and MRO was an early adopter and heavy user of the available streamlined enforcement processes.

2015-2016

Implementation of the RAI became the focus of 2015 through 2016. Pilot projects for compliance monitoring and enforcement were launched across the ERO. During this time, MRO was focused on evaluating internal controls and scoping compliance audits based on individual entity risk. Pilots were also launched for the Self-Logging Program and coordinated oversight of Multi-Region Registered Entities.

Most significant during this time, was the adoption of the Compliance Exception process. This process allows for the relatively quick resolution of minimal risk issues outside an enforcement filing. From July 1, 2014, the date that Compliance Exceptions became eligible for filing, to December 31 2016, MRO processed 125 instances of noncompliance as Compliance Exceptions.

(Continued on page 8)
Inherent Risk Assessments (IRAs) were developed for all registered entities in MRO. IRAs consider individual risk based on a registered entity’s functions, equipment, facilities, location, etc. MRO also led an initiative to gain greater alignment in IRA considerations across the ERO. Leveraging the IRA output, MRO also began developing Compliance Oversight Plans (COPs) for registered entities scheduled for a compliance audit in 2017. COPs are three-year plans that consider information MRO has obtained about a registered entity’s performance risk, based on considerations of compliance history, events, response to NERC Alerts, etc. Each COP identifies the Standards and Requirements and the compliance monitoring approach (audit, self-certification, spot check) for each calendar quarter. All entities scheduled for an audit in 2017 received a draft COP in 2016 for review and an opportunity to provide feedback to MRO.

**2017-2018**

Currently, MRO has completed IRAs for all entities on the registry through October 2016. MRO is developing COPs for all registered entities and anticipates providing draft COPs in 2017 for all Transmission Operators, Balancing Authorities, and Reliability Coordinators. COPs will be completed for other registered entities in 2018.

Streamlined enforcement processes are a part of the day-to-day process at MRO. Enforcement is reserved for significant matters. FFT, CE, and SNOP processes are fully implemented. Settlements are rare as a shared understanding of risk results in greater acceptance of enforcement determinations. Across the ERO, a Compliance Guidance Policy has been adopted to provide greater clarity to registered entities. Under the Compliance Guidance Policy, Implementation Guidance is developed by industry and provided deference by the Regional Entities. Many of the Standard Application Guides developed under the MRO Standards Committee have been endorsed by the ERO under the Compliance Guidance Policy. Additionally, Compliance Practice Guides are released to provide direction to Regional Entity staff related to CMEP practices. The first Compliance Practice Guide directs the Regional Entities to provide deference to registered entities following Implementation Guidance. This is a process that reflects the transparency and collaboration that MRO has always strived for in our CMEP efforts.

**2018 and Beyond**

As we move into the future, MRO anticipates further adjustments in our processes. We anticipate that registered entities will be HEROs with strong, self-monitored compliance programs. MRO will continue to provide clarity and support, as well as assurance through “right-sized” compliance oversight. We will continue to focus on risk identification and analysis of the bulk power system, the region, and at the individual registered entity level. Through the identification of emerging risks, and outreach with industry, MRO will provide transparency of expectations and assist with mitigation of known risks.

MRO will conduct targeted CMEP activities that are customized for each registered entity. Compliance oversight will identify monitoring methods, frequency, and scope for each monitoring activity. COPs will continue to be developed and considered “living” documents, with smaller CMEP touchpoints becoming the norm and large audits becoming rare. MRO anticipates that COPs will provide an alternative to the three-year onsite audit requirement for Transmission Operators, Balancing Authorities, and Reliability Coordinators currently required by the Rules of Procedure. Additionally, COPs will eliminate the need for an annual CMEP Implementation Plan, as registered entities will have individualized plans.

Moving forward, MRO anticipates that the Compliance Exception process will be expanded to include moderate risk issues and the FFT process will be retired. Ultimately, MRO would like to see Compliance Exceptions as a processing option regardless of the risk, but recognizes that this approach is unlikely to be adopted at this stage of mandatory enforcement. Additionally, MRO expects that the Self-Logging Program will evolve, such that noncompliance is recorded at the Regional Entity level and not submitted to NERC and FERC. The Self-Logged noncompliance would be available to NERC and FERC upon request.

**Conclusion**

Everything we do is about reliability. As we move forward, this overarching imperative informs our decision making. We will continue to lead in the evolution of the risk-based approach to compliance monitoring and enforcement. With the help of those we regulate, we will see continued improvements in addressing risks to reliability and security of the bulk power system.
Steady State of Reliability Standards?
Are we approaching a steady state for Reliability Standards? It appears that projects related to Reliability Standards are starting to slow down. The focus now is on refining the existing requirements through the Enhanced Period Review (EPR) process.

Currently the Electric Reliability Organization (ERO) has nine standards projects underway, which, with the exception of Cyber Security Supply Chain Management, are related to existing Reliability Standards:

- 2013-03-Geomagnetic Disturbance Mitigation
- 2015-9- Establish and Communicate System Operating Limits
- 2015-10- Single Points of Failure TPL-001
- 2016-02 Modifications to CIP Standards (CIP-006)
- 2016-02- Modifications to CIP Standards (V5 TAG Issues)
- 2016-EPR-01 Enhanced Periodic Review of Personnel Performance, Training, and Qualifications Standards
- 2016-02- Enhanced Periodic Review of Voltage and Reactive Standards

In addition to these current projects, there are seven Reliability Standards that have been approved by the Federal Energy Regulatory Commission (FERC) and are subject to future enforcement:

- COM-001-3 Communications and IRO-002-5 Reliability Coordination – Monitoring and Analysis, which will become effective on October 1, 2017
- BAL-002-2 Disturbance Control Standard – Contingency Reserve for Recovery from a Balancing Contingency Event and PRC-026-1 Relay Performance during Stable Power Swings, which will become effective January 1, 2018
- IRO-018-1(i) Reliability Coordinator Real-time Reliability Monitoring and Analysis Capabilities, which will become effective April 1, 2018
- TOP-001-4 Transmission Operations, which will become effective July 1, 2018.

Eleven additional Reliability Standards have been submitted to FERC and are pending regulatory approval.

As each project develops, members of MRO’s organizational group, NERC Standards Review Forum (NSRF), continue to engage with the NERC Standards Drafting Teams and NERC developers each Wednesday to gain a better understanding of the modifications and express their viewpoints. Individuals who want to be added to the NSRF distribution list should contact MRO at msq@midwestreliability.org.

Upcoming Industry Webinar on Geomagnetic Disturbance Mitigation
NERC is hosting an industry webinar on July 27, 2017, from 2:30 to 4:30 p.m. Eastern on Project 2013-03 Geomagnetic Disturbance Mitigation. This webinar will present revisions made to the Standard by the standard drafting team in response to FERC Order 830. The Standard is posted for industry comment through August 11, 2017. There are also a number of supporting documents posted with the standard on the project page.

You can find out more about the webinar, including background information and registration instructions on NERC’s website.
A great book for aspiring HEROs

Miggie Cramblit, Vice President General Counsel, Corporate Secretary and Director External Affairs

In almost every Midwest ReliabilityMatters you will find an article that mentions High Reliability Organizational (HRO) theory, which MRO has adapted as HEROs –Highly Effective Reliability Organizations. In fact our raison d’être, is to “Strive to assure each Bulk Power System owner and operator within our region is a Highly Effective Reliability Organization.”

HEROs follow five principles:

- Preoccupations with Failure
- Reluctance to Simplify Interpretation
- Sensitivity to Operations
- Commitment to Resilience
- Deference to Expertise

MRO Reads first encountered David Marx in his book Whack-a-Mole: The Price We Pay for Expecting Perfection. In Whack-a-Mole, Marx illustrates human fallibility and how we should respond to it with a series of vignettes. He categorizes mistakes as human error, at-risk behavior and reckless behavior each with an appropriate response, console, coach and punish, respectively.

In Dave’s Subs, Marx creates the fictional world of Dave, a former Wall Street securities trader, who left trading six years ago to start Dave’s Subs. Both of these books offer practical guidance for developing systems and managing people, and while Marx does not refer to HRO theory, you will find many aspects of his advice are practical applications of HRO theory.

When the book opens we are introduced to Milo, who after almost three years of making sandwiches as an “artisan” has just been given the opportunity to open and manage Dave’s sixth sub store. One day when Milo isn’t in the store, one of his employees fails to serve a gluten free bun to a customer who has celiac disease. The mistake lands the customer in the hospital, forcing her to miss her daughter’s wedding in Hawaii. Of course the customer is a high profile litigation attorney.

So begins our journey with Milo who is managing Dave’s Subs with his five employees, Alisha, Fred, Charles, Esther and Bryce, each of whom rather predictably have different aspirations and completely different backgrounds. Wild Bill, the consultant; Isabel, his wife; John, his college chum and golf partner; and even Denzel Washington, the actor, serve as the foils for the lessons Marx wants to illustrate.

The initial focus in the book is the need for good systems. As Marx notes “good human beings have to work awfully hard to overcome bad system design.” Wild Bill, a human factors investigator for the National Transportation Safety Board, teaches Milo about four concepts to designing a good system including: (1) performance-shaping factors; (2) barriers, (3) redundancy, and (4) recovery. The (Continued on page 11)
rest of the book is about accountability and managing drift from the system design.

What is particularly helpful about this book, as compared to Whack-a-Mole, is the ongoing work setting which allows Marx to explore different kinds of mistakes, why they occur, and our immediate responses. After following these five employees through their ups and downs, Milo creates a performance review process that credits first and foremost the mission of Dave’s Subs – fast and friendly service, but also recognizes intangible contributions employees make to the enterprise, such as developing a website or marketing campaign, so the entirety of the employee’s work is recognized, not just the metrics.

Throughout the book you will encounter concepts or phrases that are reminiscent of things we talk about at MRO.

We frequently say: “The hallmark of reliability in complex, real-time, interdependent systems is not that errors won’t occur, it’s that errors and operating anomalies won’t create an uncontrolled cascading event.” Marx says: “Bad events will happen.”

We say you don’t get credit for being lucky, you get credit for being good and we know the difference. Marx says: “Milo was not just questioning ‘no harm, no foul,’ but thoroughly rejecting it. Accountability should have very little to do with the actual outcome.”

We insist that even the lowest level events be analyzed following the HRO principle of “reluctance to simplify” and are quick to publish Lessons Learned. Marx quotes Dave as saying: “Getting at the causes behind these events helps us really look at and fine-tune our systems....”

For those of you aspiring to lead your company to becoming a HERO, this book will give you some very practical guidance to apply in any setting.

Thanks to Dr. James Merlo, NERC’s Vice President and Director of Reliability Risk Management, for recommending these books!

4 Id., at p. 296.
5 Id., at p. 139.
6 Id., at p. 187.

(Continued from page 10-MRO Reads)

GridSecCon 2017

October 17-20, 2017 | Saint Paul, Minnesota

Registration is now open!

The North American Electric Reliability Corporation (NERC) holds the annual Grid Security Conference (GridSecCon) series to bring together cyber and physical security experts from industry and government to share emerging security trends, policy advancements, and lessons learned related to the electricity industry.

The seventh annual GridSecCon is in the Midwest Reliability Organization region on October 17-20, 2017, at the InterContinental Saint Paul Riverfront in Saint Paul, Minnesota. The conference spans four days and includes training, general sessions, utility tours, and threat briefings at the classified and for official use only levels.


Location:
InterContinental St. Paul Riverfront Hotel
11 Kellogg Blvd. E.
Saint Paul, MN 55102

More information can be found HERE.
Responding to SCADA Malware May Require Stepping Up our Game

Jodi Jensen, Operations Support Manager and Senior SCADA Specialist, Western Area Power Administration

I’m hoping this article will spark an industry conversation on cyber security implementation strategies for addressing the escalating threat posed by SCADA Malware. On June 13, 2017, NERC released an Alert Advisory entitled “Modular Malware Targeting Electric Industry Assets in Ukraine” that contained recommendations to the industry. This article takes a strategic look at implementation options and tradeoffs in responding to NERC’s recommendations.

Limit Privileged Access

Optimal SCADA security would include limiting privileged SCADA access to local users and administrators. However, remote access is often desired because it allows support to be provided remotely. Although utilities want deep bench strength in their administrators that can maintain SCADA systems, economic benefits entice organizations to leverage IT staff outside of the local facility as opposed to hiring local administrators. Options to consider include the following. 1) Hire a deep bench of local administrators, so remote privileged access is not required. This staff can perform additional duties associated with increasing compliance and cyber security responsibilities, along with their key responsibilities in the highly specialized area of SCADA reliability. 2) Limit privileged remote access by establishing a network connection that local administrators or operators can physically disable when remote support activity is not occurring. 3) Limit privileged access locally by implementing separation of duties and establishing a process where a few local administrators will enable privileged accounts for other administrators only during support activity. 4) Perform periodic evaluations of all privileged accounts to determine which are still needed.

Implement Two-Factor Authentication

Some of the implementation decisions for two-factor authentication include where to locate authentication infrastructure and associated support responsibilities. Optimal SCADA Security would include dedicating equipment for two-factor authentication for SCADA with infrastructure located directly on the SCADA network. However, authentication from an external security center is often desired for efficiency and monitoring. A few options to consider include the following. 1) Purchase the extra equipment to allow for the location of dedicated two-factor authentication systems.
directly on the SCADA network to mitigate the potential for remote revocation or manipulation of SCADA access from an external point of infiltration. 2) Utilize your deep bench of local administrators to support and maintain the two-factor authentication infrastructure locally. 3) Push authentication activity logs to a centralized security center through a unidirectional gateway or tap, allowing centralized monitoring and aggregation without the need to introduce a new network path into the SCADA network and the associated enlargement of the cyberattack surface.

**Monitor network traffic**

Some of the implementation decisions for monitoring systems include where to locate monitoring infrastructure and associated support responsibilities. Optimal SCADA Security would include local monitoring, as well as remote monitoring and aggregation. A few options to consider include the following:

1. Purchase local monitoring equipment to allow local administrators to continue to have visibility during cyber incidents when isolation of the local network is required. Isolation could limit the ability for alerts to get to the security center, and conversely for local administrators to view monitoring information from the security center.

2. Push monitoring information to a centralized security center through a unidirectional gateway or tap, allowing centralized monitoring and aggregation without the need to introduce a new network path into the SCADA network and the associated enlargement of the cyberattack surface.

3. Iteratively build, test, and tune monitoring capability, employing new IT technologies, such as network heuristics, to identify traffic deviations.

**SCADA configuration information protection**

Sophisticated SCADA malware is targeted and autonomous. Therefore, effective attacks require the malware to embody a deep knowledge of the target network and SCADA protocols. Gaining accessibility to SCADA configuration information is one of the most significant factors in an adversary’s ability to carry out an attack using the new modular malware. Optimal SCADA configuration information protection would include housing SCADA configuration files on a locally protected network with a redundant backup and recovery strategy in place, to include periodic offline backups. However, centralized information repositories are desirable for efficiencies in maintaining a centralized compliance program. A few options to consider include the following:

1. Utilize your deep bench of local administrators to support the locally protected server housing the SCADA configuration information and the extra duties handling access to the protected information.

2. Provide access to external staff through a tightly controlled process that requires strong encryption.

3. Maintain the master copy of all SCADA configuration information locally so local administrators can continue to have accessibility during cyber incidents that require network isolation.

4. Perform periodic evaluations of SCADA information housed externally to validate the need and security of external storage.

**Other recommended cyber security controls**

Implementation of security controls such as application whitelisting, maintaining YARA rules, patch management, and digital hash validation, can provide additional protection from modular SCADA malware. Optimal SCADA Security would include resourcing these activities with local infrastructure and local administrators. However, utilization of remote IT staff is often desired when staffing constraints exist or expertise is limited. 1) Utilize your deep bench of local administrators to support these systems and activities to the degree possible. 2) When remote support is essential, establish a network connection that local administrators or operators can physically disable when remote support activity is not occurring.

**Conclusion**

Local infrastructure and local administrators are increasingly important to the viability of maintaining an optimal cyber security posture. While most of the strategies outlined above require additional workload, these extra duties can be achieved by hiring a few students or recent graduates that will eventually grow into your highly specialized SCADA administration specialists. Increasingly, the industry focus is on cyber security response activities. Having a deep bench of local SCADA administration professionals maintaining SCADA system reliability, while effectively defending and responding to cyberattacks, might be the best value proposition in achieving an optimal cyber security posture.
Electricity Information Sharing and Analysis Center

In May 2017, I was invited to the Electricity Information Sharing and Analysis Center (E-ISAC) in Washington D.C. to listen and learn about insights that are impacting the North American grid. While in D.C., I made connections with the agency heads that run the National Cybersecurity and Communications Integration Center (NCCIC). I had first heard about the NCCIC when I was finishing up my Graduate degree at the University of Minnesota in Security Technologies and had always wanted to visit.

I joined other critical infrastructure security professionals in touring the watch floor of the NCCIC, which is the epicenter of U.S. Cyber Intelligence integration. The United States Computer Emergency Readiness Team website describes NCCIC as follows:

“The NCCIC serves as a central location where a diverse set of partners involved in cybersecurity and communications protection coordinate and synchronize their efforts. NCCIC’s partners include other government agencies, the private sector, and international entities. Working closely with its partners, NCCIC analyzes cybersecurity and communications information, shares timely and actionable information, and coordinates response, mitigation and recovery efforts.”

Of note, the tour occurred during an actual incident and I was able to see firsthand how the various agencies integrate and operate.

One of the most intriguing aspects of my visit was that the NCCIC offers significant opportunities to integrate the many agencies and organizations working to secure the grid. I noted many people from the various agencies on-site working together and communicating in a collaborative manner. Sometimes, a public facing report is provided as an outcome from this integration and we noted one of those most recently with the release of the CrashOverride Malware report. It’s refreshing to see first-hand the coordination and back-end communication that helps secure our nation’s infrastructure. This is a valuable reminder that companies facing future incidents will need to coordinate with other agencies to resolve the issue.

Please stay tuned for more information and details about how the E-ISAC, Electric Sector and the NCCIC are working together to enhance the nation’s security.

MRO Security Advisory Council Holds Two Webinars in June

The MRO Security Advisory Council (SAC) hosted two webinars during the month of June 2017.

The first webinar, *Exploring the Unknown ICS Landscape*, was held on June 2 and was presented by Mr. Robert M. Lee.

Mr. Lee is the CEO and founder of the ICS (Industrial Control Systems) cybersecurity company Dragos, Inc. He is also a national cybersecurity fellow at New America who focuses on critical infrastructure policy issues and the course author of SANS’ ICS515, where he teaches ICS security personnel how to actively defend and respond to threats in the ICS.

This presentation discussed unique research on ICS software, malware, and the consequences of poor operational security. The thesis underlying this research is there is a wealth of useful information surrounding ICS not recognized by the traditional IT cybersecurity industry. Mr. Lee walked through proven methodologies, and showed real-world findings and conclusions of what this means to the electric industry.

Slides from the webinar may be found [here](#).

The second webinar, *Securing SCADA*, was held

(Continued on page 16)
EVENT DETAILS:
Please join us for MRO’s 2017 Security Conference, which is preceded by a day of technical training designed to provide security professionals the tools to address some of the many security challenges facing the electric utility industry today. All security professionals, SMEs, and power system engineers from registered entities in the MRO Region are encouraged to attend.

TECHNICAL TRAINING
September 27, 2017 │ 8 a.m. to 4 p.m.
“Threat Hunting and Incident Response for Environments”
Ben Miller from Dragos, Inc., will provide an introduction to threat hunting and incident response for Industrial Control System environments. This training is sponsored by the MRO Security Advisory Council. We will review the business and security use cases of when and why threat hunting is valuable to organizations. These concepts will be applied to corporate environments and industrial environments such as transmission and distribution control facilities, or generation distributed control systems. This session will serve as an introduction to key concepts and provide a framework to develop active defenses, and will also include demonstrations of tools and tactics that can be immediately applied.

SOCIAL NETWORKING EVENT
September 27, 2017 │ 5 p.m. to 7 p.m.
Training and conference attendees are invited to join us at the Hampton Inn & Suites in Saint Paul for a social networking event. Appetizers and beverages will be provided.

SECURITY CONFERENCE
September 28, 2017 │ 8 a.m. to 5 p.m.
This conference is designed to provide clarity by expanding security awareness and strengthening cyber and physical security through information shared by experts within the security industry, as well as analysis of real-world security lessons and best practices. All security professionals, subject matter experts, and power system engineers from registered entities in the MRO Region are encouraged to attend.

Topics of Interest:
- Executive Security Perspectives
- Physical Security
- Cyber Security
- Electricity Subsector Coordinating Council (ESCC) Update
- Electricity Information Sharing and Analysis Center (E-ISAC) Update
- World War II Enigma Machine (encore performance)
- Exploring the Unknown ICS Threat Landscape

REGISTRATION AND LODGING:
You may register for one or both of these events. Registration is subject to review and approval, with preference given to MRO registered entities. A block of rooms has been reserved at the Hampton Inn and Suites at a rate of $169/night. The room block ends on August 28, 2017.

Please email securityconference@midwestreliability.org for registration information.
on June 29 and was presented by the following individuals:

- Andrew Ginter, VP Industrial Security, Waterfall Security
- Jodi Jensen, Operations Support Manager, Western Area Power Administration, MRO SAC Member
- Tyler Stinson, Substation Communications Engineer, Xcel Energy, MRO SAC Member

The presentations provided information on how to better secure SCADA systems, along with a deeper dive into securing SCADA and substation networks.

Andrew’s presentation focused on *SCADA Security – What’s Broken and How to Fix it*. Two MRO SAC members with expertise in SCADA security, Jodi Jensen and Tyler Stinson, provided a brief overview on *SCADA Network Security*, and *Substation Network Security*.

Slides from the webinar may be found [here](#).

---

### Joint Study on Bulk Power System Restoration and Recovery

**Bill Kunkel, Principal Operations Engineer**

In January 2016, FERC and NERC published the [FERC-NERC, Regional Entity Joint Review of Restoration and Recovery Plans Report](#). This study assessed entities’ plans for restoration and recovery of the bulk power system following a widespread outage or blackout. The report identified several issues that were beyond the study’s scope. One of the areas identified for further study was the potential impact of the loss of Supervisory Control and Data Acquisition (SCADA) systems on bulk power system restoration.

Last fall, FERC, NERC and the Regional Entities initiated a joint study called Planning Restoration Absent SCADA or EMS (PRASE), which focuses on the potential impact of the loss of SCADA, Energy Management System (EMS), or Inter-Control Center Communications Protocol (ICCP) functionality on system restoration and the manner in which such impact could be mitigated. The study team gathered information from eight volunteer registered entities (the participants),
from different regions and with significant bulk power system responsibilities. On June 9, 2017, the results from the Joint Study Report: Planning Restoration Absent SCADA or EMS (PRASE) were published. In this second report, the joint study team noted numerous practices employed by individual participants that may be of value to other bulk power system owners and operators. While each practice may not be universally appropriate or possible, the joint study team recommends that entities consider the practices, or variations thereof, into the entity’s operations as appropriate.

The joint study team found that all participants have made significant investments in their SCADA and EMS infrastructures, including leveraging redundancies to increase availability and functionality. The participants indicated that they would remain capable of executing their restoration plan event without SCADA/EMS availability. They acknowledged, however, that completion of all restoration steps would be more time consuming and more involved under such conditions, especially those steps requiring a larger degree of coordination and those steps performed during later stages of the restoration process.

All contacted entities agreed to participate in the study, and without exception, were exemplary in their cooperation with the joint study team, sharing the detailed technical rationale behind implementation of their system restoration plans in the absence of SCADA or EMS. The joint study team commends the participating entities for their open and active contributions.

The joint study team developed five recommendations in the report that are appropriate for all entities responsible for system restoration.

1. **Planning for backup communications measures.**
   Entities should review and refine as necessary their backup communications measures and capabilities to ensure that they can be depended on to provide effective means of communications in the event of the loss of normal communications means during system restoration absent SCADA or EMS.

2. **Planning for personnel support during system restoration absent SCADA.**
   Entities should review and refine their human resource operations support measures as needed to support the field and control room personnel necessary for system restoration absent SCADA.

3. **Planning backup power supplies for an extended period of time.**
   Due to the expected increase in time to accomplish system restoration absent SCADA/EMS functionality, entities should review and refine as necessary their existing provisions for backup power resources at restoration path substations and other locations identified as priority or critical in system restoration plans, to ensure they are available for an extended period of time beyond the normal expectation from battery backups.

4. **Analysis tools for system restoration.**
   Recognizing that the absence of SCADA/EMS functionality results in loss of State Estimator and Real-Time Contingency Analysis, applicable entities should review and refine as necessary other analysis tools for use (e.g., use of offline power system analysis tools, phasor measurement unit data) especially during the later stages of restoration.

5. **Incorporating loss of SCADA or EMS scenarios in system restoration training.**
   Applicable entities should, as part of their system restoration training, practice implementation of restoration plan steps absent SCADA/EMS functionality or other data sources, including incorporating the insights found.

---

_You can have the nine greatest individual ballplayers in the world, but if they don't play together, the club won't be worth a dime._

- *Babe Ruth, Baseball Player*
COMPLIANCE OVERSIGHT PLANS
Taking Risk-Based Compliance Monitoring to the Next Level

Sara Patrick, VP Compliance Monitoring and Regulatory Affairs and Jim Morales, Senior Compliance Auditor

With the completion of Inherent Risk Assessments (IRAs) for all registered entities in the MRO region, the MRO Compliance Department has been focused on developing three-year Compliance Oversight Plans (COPs). This is the next step in our journey to fully implement risk-based approaches in our compliance monitoring oversight.

IRAs and COPs are both individualized for each entity, with the IRA being one of the inputs to the COP. While IRAs focus on an entity’s inherent risk based on certain characteristics such as size, operations, equipment, functions performed, and unique configurations; COPs include risks associated with an entity’s compliance history including factors such as mitigation efforts, risk level of past noncompliance, and ability to self-monitor compliance and assess risk of noncompliance. COPs also consider events and associated compliance concerns, if any, as well as an entity’s response to NERC Alerts.

MRO is developing COPs for all registered entities starting with the Transmission Operators (TOPs), Balancing Authorities (BAs), and Reliability Coordinators (RCs). All entities registered for these functions will receive a COP in 2017. COPs include a three-year roadmap noting which Reliability Standards and Requirements are subject to audit or self-certification in each quarter of the three-year period. MRO’s practice is to provide a draft COP for review and feedback by the registered entity prior to issuing a final version. The feedback we have received to date has been varied and primarily focused on individual Reliability Standards and Requirements.

Some TOPs, BAs, and RCs may be subject to an audit each year, while others may be subject to an audit only once or twice during the three-year timeframe. MRO anticipates that when there are multiple audits scheduled over a three-year period, only one of the audits will include an on-site visit since the NERC Rules of Procedure (ROP) require one on-site visit every three years for these functions. MRO further anticipates that in the future, COPs will be an alternative to the three-year onsite audit requirement in the ROP. For entities not registered for one of these three functions (TOP, BA or RC), there may or may not be an audit component identified in the COP, with some of these registered entities only subject to audit once during a five-year period. COPs are “living” documents that require review on a periodic basis. Prior to scheduled compliance monitoring, MRO will assess whether there have been any changes with regard to an entity’s compliance history, regional or ERO-wide compliance trends, or newly effective Reliability Standards and Requirements that pose risk for an individual registered entity.

This assessment may result in changes to “In-Scope” Reliability Standards and Requirements to be monitored. When an audit is scheduled, MRO will continue to provide formal Audit Notification Letters (ANL) that detail the audit process, expectations, and identify those Reliability Standards and Requirements in scope for each audit. As we move forward and fully implement risk-based approaches in our compliance monitoring oversight, our goal is to have an improved shared understanding of risks and focus resources for all involved in CMEP activities on those risks.

The following Tips and Lessons Learned have been compiled by MRO staff during the conduct of compliance audits, mitigation plan reviews, enforcement actions, and event analysis. If you would like clarification on a particular topic, please contact jr.mitchell@midwestreliability.org.
FINANCE AND ADMINISTRATION

Sue Clarke, VP Finance and Administration

**Year-to-Date Financials**
Year-to-date, the 2017 budget results are within 1.5% of budget. We expect on-budget performance by year-end.

**ERO 2018 Business Plan and Budget Timeline**
The 2018 MRO Business Plan and Budget, which was previously reviewed with board members and posted for stakeholder comment, was approved by the MRO Board of Directors on June 22, 2017.

The budget includes a 30 day retained reserve. The board found that the 2018 budget is sufficient for MRO to meet its delegated responsibilities. The final version of the business plan and budget was posted on June 23, 2017, and will be submitted for approval to the NERC Board of Trustees at its August 9, 2017 meeting.

Subsequently, NERC will file the business plans and budgets for NERC and the eight Regional Entities with the Federal Energy Regulatory Commission.

**Culture and Talent Management**
This summer, MRO staff will participate in various training opportunities, both required and developmental. MRO’s executive training committee is finalizing staff, managerial, and executive workshops. These training opportunities enhance skills and knowledge, and help fulfill necessary continuing education requirements. The committee’s goal is that every year staff is provided opportunities to stay current in technology, industry, and related fields of work.

Examples of topics on this year’s schedule are writing and editing skills, impactful leadership, and staff engagement. Other offerings will be a part of the MRO brown bag series for standards training, cybersecurity, meeting procedures, and other topics.

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

Questions regarding accounts payable or receivable should be directed to Regina Davis, Accountant and HR Generalist.
Measuring the Cost of Inaction

Jessica Mitchell, Stakeholder Relations and Communications Principal

The Elevating Ethics column in the November 2016 Issue of this publication featured the Wells Fargo banking scandal, arguably one of the largest and most notable business scandals of the last decade. The scandal involved thousands of Wells Fargo employees, who under pressure to meet unrealistic sales targets, had opened millions of unauthorized customer bank and credit card accounts to boost their sales numbers. The decade-long scandal was finally brought to light in 2016 and ended up costing Wells Fargo millions of dollars in fines and restitution. Two of the bank’s top executives, including then Chairman and CEO John Stumpf, lost their jobs as a result of the scandal and took a financial hit when Wells Fargo clawed back $75 Million of their compensation.

The article from last November describes several lessons that can be learned from this event, like the importance of cultivating an ethical business culture, having strong controls in place to prevent fraud and employee misconduct, and the significant costs of inaction. I’d like to focus more on this last lesson here…the significant costs of inaction.

Wells Fargo management, while aware of its employee’s misconduct, failed to take the appropriate action to put a stop to the behavior. But Wells Fargo management wasn’t the only party to fall flat. According to a recent article in the New York Times, the regulator in charge of overseeing the bank’s activities also failed to act on several red flags that could have brought the scandal to light much, much sooner. The article states that the Office of the Comptroller of Currency (OCC), responsible for regulating and supervising all national banks in the United States, “admitted that its oversight of Wells Fargo was ‘untimely and ineffective.’” The OCC directed its Enterprise Governance Division to perform an internal review of its Wells Fargo oversight to identify any supervision gaps and lessons learned.

This past April it issued its final report on the matter, which highlighted areas where the OCC’s oversight of Wells Fargo was ineffective and failed to recognize early warning signs.

The report found that in 2009, the OCC had identified an issue with Wells Fargo’s complaint management system and issued a Matters Requiring Attention (MRA) to Wells Fargo, which as of December 2016 had not yet been corrected. Even though over this seven-year period the OCC could have escalated the matter and pursued further corrective actions, it did not. The report also revealed that the OCC was aware of issues with the bank’s sales practices since at least 2010, and admitted that because of deficient supervisory and oversight practices, it failed to comprehensively assess and identify the root causes of Wells Fargo’s many complaints and whistleblower cases. Had the OCC taken the necessary corrective actions and exercised more rigorous oversight of Wells Fargo, the fraudulent activity may have been discovered sooner and mitigated without such significant financial repercussions.

(Continued on page 21)
Inaction also appears to be a primary factor of the catastrophic Grenfell Tower fire in London in mid-June that killed at least 80 people. Evidently both the building’s owner and British regulators were aware of potential fire safety hazards, but failed to take the necessary actions to prevent the devastating blaze. The Guardian reported that residents of the Grenfell Tower had previously raised concerns to the building management company “over the placement of boilers and gas pipes, the absence of a building-wide fire alarm or sprinkler system, and piles of rubbish being dumped and causing a fire risk.” Their concerns were ignored.

While the building’s owner may ultimately bear responsibility for the event, a New York Times article also lays blame on British regulators for placing cost concerns over public safety. It asserts that the combustible materials used in the building’s façade have long been known to be a fire hazard and are prohibited from use in high-rise buildings in the United States and many other European countries. While other countries chose to add regulations prohibiting the use of such materials, the article states that British authorities ignored the potential risk—in part because of the high cost to install more fire-retardant alternatives, but also because of a political environment aiming “to free businesses from the burden of safety regulations.”

Just as more rigorous oversight could have minimized the scale and financial impact of the Wells Fargo scandal, more stringent fire safety regulations could have minimized the deadly impact of the Grenfell Tower fire.

Both of these events clearly demonstrate that the cost of inaction is not only high, it’s avoidable. Even though a known risk may appear insignificant, a failure to act on it can lead to devastating consequences—financial implications, loss of reputation and public trust…even loss of life.

According to Drs. Karl E. Weick and Kathleen M. Sutcliffe,1 These types of failures are rare in High Reliability Organizations (HROs). HROs focus on failures rather than successes—reliability rather than efficiency. The HRO Principles empower individuals to take action.

For example, had Wells Fargo been preoccupied with failure, it would not have ignored the many small instances of fraud that led to a much larger event.

Had the OCC not oversimplified its interpretations of Wells Fargo whistleblower cases, it would have dug deeper into the root causes and unearthed the scandal sooner.

The owners of Grenfell Tower lacked a sensitivity to operations and allowed a hazardous environment to contribute to an avoidable catastrophe.

And finally, British authorities did not defer to expertise, or heed the warnings of local fire safety experts.

Former U.S. President John F. Kennedy said “There are risks and costs to action. But they are far less than the long range risks of comfortable inaction.”

Taking the necessary actions to protect the reliability of the North American bulk power system is our collective responsibility. By applying the HRO theory, we can each strive to be Highly Effective Reliability Organizations, or HEROs.

Compliance Update

Compliance Oversight Plans (COP)

The MRO Compliance Department is developing COPs for all registered entities. This process is maturing, and MRO received helpful suggestions for enhancements and feedback from registered entities that have received a COP in 2017. MRO has begun sharing COPs for those entities scheduled to be audited in 2018. Between May and September, those entities scheduled to be audited in 2018 will receive draft COPs for review and feedback to MRO.

2017 Compliance Audit Status

MRO is leading six Compliance Audits in 2017 and has completed three of these six as of June 30, 2017. MRO is also participating in multi-Regional coordinated oversight as an Affected Regional Entity in four Compliance Audits in 2017. MRO’s 2018 Audit Schedule has been posted to the website, which identifies the registered entities scheduled for audit in 2018 and indicates whether the audit will be conducted on-site at the registered entities’ facilities, or off-site at the MRO offices.

Risk Assessment and Mitigation Update

HEROs Update

MRO’s Risk Assessment and Mitigation Department continues to answer questions from registered entities in the MRO Region and regularly attend Mid-Continent Compliance Forum (MCCF) Critical Infrastructure Protection (CIP) meetings to respond to registered entity questions. MRO staff is also closely following the CIP V5 Revisions, CIP-012 (Communications between Control Centers), and TPL-001-4 (Transmission Planning) Standard Drafting Teams. MRO continues to encourage registered entities to submit technical questions via email to MRO at HEROS@midwestreliability.org.

Compliance Severity Index

In order to evaluate its progress toward a key reliability goal of less severe events and violations, MRO uses the Compliance Severity Index (CSI) to represent the total risk that all instances of noncompliance present to the reliability or security of the Bulk Power System (BPS) in the MRO Region. The CSI is calculated using the Risk Determination and Discovery Method for each non-compliance. 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.

MRO Compliance Monitoring and Enforcement Program

Figure 1: Total Compliance Severity Index by Discovery Year

<table>
<thead>
<tr>
<th>Year</th>
<th>Minimal</th>
<th>Moderate</th>
<th>Serious</th>
</tr>
</thead>
<tbody>
<tr>
<td>2007</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
</tr>
<tr>
<td>2008</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
</tr>
<tr>
<td>2009</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
</tr>
<tr>
<td>2010</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
</tr>
<tr>
<td>2011</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
</tr>
<tr>
<td>2012</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
</tr>
<tr>
<td>2013</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
</tr>
<tr>
<td>2014</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
</tr>
<tr>
<td>2015</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
</tr>
<tr>
<td>2016</td>
<td>29%</td>
<td>3%</td>
<td></td>
</tr>
<tr>
<td>2017</td>
<td>3%</td>
<td>3%</td>
<td>3%</td>
</tr>
</tbody>
</table>

% of Risk Determinations Completed

Highest Risk Requirements

Since working with the CSI, it has become apparent to MRO that changes to Reliability Standards associated with projects like CIP Version 5 (Project 2014-02) and TOP/IRO (Project 2014-03) have caused certain requirements to shift (Continued on page 23)
to or be combined with other requirements, or even other Reliability Standards. Therefore, MRO staff undertook an effort to evaluate the root causes of noncompliance processed in the MRO Region in order to map the historic instances of noncompliance into the current equivalent Reliability Standards and requirements. This allows the same risk associated with varying instances of noncompliance to be analyzed, regardless of new Reliability Standards or revisions. Figure 2 provides the 15 highest risk requirements that have a history of noncompliance, based on the Total CSI.

Risk Determinations

Eighty-one percent of instances of noncompliance processed by MRO from 2007 to June 30, 2017, were Minimal Risk. (See figures 3 and 4.)

Noncompliance Trends and Statistics

Registered Entity Responsibility

MRO staff trends Self-Reports and registered entities’ acceptance of responsibility for violations. Of all violations filed with regulatory authorities, registered entities have accepted responsibility for the violation 94% of the time. This, combined with the percentages of Self-Identified violations, points to strong compliance commitment among registered entities in the region.

Figure 2: 15 Highest Risk Requirements based on Total Compliance Severity Index (2007-June 30, 2017)

Figure 3:

Figure 4:

---

COMPLIANCE AND ENFORCEMENT DASHBOARD

Breakdown of all CIP versus Non-CIP Possible Instances of Noncompliance by Year Discovered and Reported to NERC as of June 30, 2017.

Compliance Exceptions

MRO processed 146 findings as Compliance Exceptions from July 1, 2014, the date on which Compliance Exceptions became eligible for filing, to June 30, 2017, (83-CIP and 63-Ops and Planning); of the 146 Compliance Exceptions, 96 were Self-Identified.

Discovery Method Detail (June 18, 2007 - June 30, 2017)

Status of Alleged and Confirmed Instances of Non-Compliance

Noncompliance Trends

24 - Midwest Reliability Matters, July/August 2017
Compliance culture, including accepting responsibility, is an important aspect in overall governance of effective compliance. MRO staff believes that the compliance culture is strong for registered entities in the MRO region and demonstrates the MRO entities’ willingness to accept, and learn from, discovered noncompliances in order to prevent future non-compliance. In the past, MRO experienced a peak in Self-Identified issues correlating to the annual Self-Certification period. With the change in approach to Self-Certification, there is no apparent trend in timing of Self-Identified issues and this may reflect registered entities’ efforts to operationalize compliance by strengthening their own self-monitoring management practices.

Since 2007, registered entities accepted responsibility for approximately 94% of instances of noncompliance filed with NERC, did not contest responsibility for 5% of cases, and neither admitted nor denied responsibility with regards to noncompliance for 1% of cases.

For questions on this CMEP report:
Compliance: compliance@midwestreliability.org
Enforcement: enforcement@midwestreliability.org
Risk Assessment & Mitigation: HEROS@midwestreliability.org

1 Self-Identified instances referenced in this report include instances reported to MRO by Self-Report, Self-Certification, and/or Self-Log.
IMPORTANT INDUSTRY NEWS AND EVENTS

NATIONAL/INTERNATIONAL NEWS

FERC Commissioner Collette Honorable Departs at Term End
Washington, D.C.—FERC Commissioner Collette Honorable’s term expired on June 30, 2017. Read her departure message, or listen to the podcast as she reflects on her term.

Trump picks Jones Day lawyer to chair FERC
Washington, D.C.—President Trump announced that he plans to nominate Kevin McIntyre, an energy lawyer at the firm Jones Day, to chair the Federal Energy Regulatory Commission. Read more.

White House Announces Intent to Nominate Richard Glick to FERC

Parker and Peterson Resign from NERC Board
Atlanta—Deborah S. Parker was named quality and reliability leader for General Electric Renewable Energy’s Onshore Wind Business, effective July 10. Parker was appointed to the NERC Board in 2016.

Kenneth G. Peterson was named chair of the BC Hydro Board by the Cabinet of the Government of British Columbia on July 20. Peterson has served on the NERC Board since 2006.

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 Security Conference
Sept 28—Please join us for MRO’s 2017 Security Conference, which is preceded by a day of technical training designed to provide security professionals the tools to address some of the many security challenges facing the electric utility industry today. Read more about the conference on Page 15 of this publication.

NERC Annual Grid Security Conference
Oct 17-20—NERC’s annual Grid Security Conference (GridSecCon) is scheduled for October 17-20, 2017, in Saint Paul, Minnesota. The conference brings together cybersecurity and physical security experts from industry and government to share emerging security trends, policy advancements, and lessons learned related to the electricity sub-sector. Read more and register here.

MRO Fall Reliability Conference
Oct 25—Save the date for MRO’s Fall Reliability Conference planned for October 25, 2017, in Saint Paul, Minnesota. The conference will address bulk power system operational and planning-related matters in the region. More information will be available soon here.

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

Due to these new appointments, Parker and Peterson have resigned from the NERC Board of Trustees. NERC is coordinating recruitment of two new trustees through Russell Reynolds Associates. To submit a candidate or receive a full position description, contact Larry Klock or Jennifer Rockwood.

Grid Resilience to Severe Weather and Protection System Performance Improved; Risks from Cyber, Physical Security Increased
Atlanta—NERC’s State of Reliability 2017 report reviews past performance of the bulk power system, examines the state of system design, planning and operations, and the ongoing efforts by NERC and industry to continually improve system reliability and resiliency. Read the Announcement and State of Reliability 2017 Report.

REGIONAL NEWS

Will Kaul retires as Great River Energy’s Vice President and Chief Transmission Officer
July 13, 2017—Will Kaul has formally retired from Great River Energy, where he served as vice president of transmission since the company’s founding in 1999. Read more.

Minnesota regulators approve Xcel’s 1,550 MW wind expansion
July 10, 2017—The Minnesota Public Utilities Commission last week approved Xcel Energy’s plan to expand wind resources in the upper Midwest, including 1,550 MW of new resources the utility says could save consumers billions in fuel costs. Read more.
CONTACT LIST*
Main Phone: 651-855-1760
Main Fax: 651-855-1712
Web: www.midwestreliability.org

General & Executive
Dan Skaar, President and CEO (1731)
Miggie Cramblit, VP General Counsel, Corporate Secretary and Director External Affairs (1721)
Jessie Mitchell, Stakeholder Outreach and Communications Principal, Assistant Corporate Secretary (1733)
Carolina Margaria, Administrative Assistant (1739)

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

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

Compliance
Sara Patrick, VP Compliance Monitoring (1708)
Desirée Sawyer, Compliance Administrator (1730)

Mitigation and Standards
Richard Burt, VP Risk Assessment, Mitigation and Standards (1714)
Cynthia Kneisl, Risk Assessment and Mitigation Administrator (1734)
Dana Klem, Standards, Certification and Registration 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@midwestreliability.org

EMPLOYEE NEWS
Richard Quest, Principal Systems Protection Engineer, has announced that he will retire from MRO later this fall. Rich has been with MRO for over five years and has made significant contributions to protection systems-related matters in both MRO and ERO-wide. Please join us in wishing Rich the very best in his retirement!

On Saturday, July 15, a team of MRO staff and family members participated in the Insane Inflatable 5K—made up solely of inflatable obstacles! The event is sponsored by the American Cancer Society to benefit its Relay for Life movement.

ABOUT MRO
MRO is a non-profit organization dedicated to ensuring the reliability and security of the bulk power system and operates under delegated authority from regulators in the U.S. and through other arrangements in Canada. Additional information can be found on our website at www.midwestreliability.org.

NOT A MEMBER YET?
MRO membership is voluntary and free of charge. Members have input on key business matters, are eligible to participate in MRO organizational groups and on the board of directors, are involved in North American-wide assessments and policy development, and can broaden their network of industry peers. To apply for membership, visit our website or call 651-855-1760.

MRO Calendar of Upcoming Events
- August 1: Operating Committee Meeting
- August 1: Security Advisory Council Meeting
- August 2: Planning Committee Meeting
- August 3: Joint Compliance and Standards Committees Meeting
- Sept 14: MRO Board of Directors Meeting
- Sept 27: Security Conference Training
- Sept 28: Security Conference
- Sept 29: Security Advisory Council Meeting

Visit the Meeting Calendar on MRO’s website for more details.