CELEBRATING 10 Years

— A Special Anniversary Issue —
A Note From the Editors:

2017 marks MRO’s tenth year in business and we continue to celebrate. Since inception, the staff at MRO have maintained a strong focus on regional reliability of the bulk power system and this means we have continuously looked to reduce the “administrivia” and increase reliable operations. We know reliable operations are not perfect operations. And in keeping with that, we have sought to be proportional in our regulatory responses, favoring investments in reliability over penalties. We have also urged our registered entities to apply High Reliability Organization (HRO) principles as a framework for achieving highly reliable operations. You will see references to these concepts throughout this publication.

Over the past ten years, this newsletter has grown from a two-page report to what Dan Skaar fondly calls our bimonthly “magazine.” We have over 1,000 subscribers from throughout the U.S. and Canada, including individuals from registered entities, regional entities, NERC and state and federal regulators, well as people who work for vendors and consultants.

This issue coincides with our Fourth Annual Security Conference so it is especially focused on cybersecurity. In the newsletter, you will find both practical information and recommendations on how you can improve your cybersecurity posture, as well as discussions about how cybersecurity standards and our regulatory framework need to evolve.

As we embark on our second decade, with your help, we look forward to another ten years of success! Please take time to fill out this survey about this newsletter.

Thank you,
Jess Mitchell and Miggie Cramblit
As MRO recognizes its ten-year anniversary as a cross-border reliability region, maybe we should pause to really think about what that means.

FERC designated MRO as a Regional Entity under Section 215 of the Federal Power Act in 2007. Soon after, we entered into similar agreements with Manitoba and Saskatchewan. As I reflect on the last ten years, I can’t help but think about what it means to be a Regional Entity. What is a Region? Are Regions important to the construct of the Electric Reliability Organization and our regulatory model? And if so, why?

What is a Region? We might understand what a Region is from our history. Our industry grew-up regionally, since the 1940s. The first system handshake between systems created the concept of a Region, and, the need to define the technical parameters to manage the handshake were the beginnings of an early structure for regional reliability.

Today, we have dozens of Reliability Standards overseeing handshakes by requiring coordination between transmission and generator owners and operators, coordination between transmission planners and planning coordinators, and between reliability coordinators and transmission operators. This defines reliability for a Region. In fact, the reliability across Regions, that is the entire Eastern Interconnection, is predicated on handshakes between systems. This is especially important for cybersecurity, where handshakes need to be trusted.

We might also understand a Region to be a community centered on shared reliability. It’s our neighborhood. We know and understand our neighbors. We all share the same objective of high reliability—working together to keep the lights on. High reliability depends on a sense of mindfulness, you need to understand your neighboring system in the context of your own system. And, this understanding is at the facility level and it’s the physics—this is where investment decisions are made—this is where blackouts are prevented.

The recent Department of Energy staff report on Electricity Markets and Reliability defined Regions as the Balancing Authorities (BAs) to consider “[i]ssues confronting the Bulk Power System [that] vary widely across regions.” MRO’s BAs are Southwestern Power Pool and MISO in the U.S., and in Canada, SaskPower.

When I think of a Region, I think of it as the hub of Reliability. As a Regional Entity, we are not simply a Compliance Enforcement Authority; we are a problem-solver alongside of you. Part of the community. Joined at the hip. Working together towards a shared mission of public service.
Our business is reliability. As part of the Electric Reliability Organization, we are in the business of ensuring reliability. We have long since sought, and continue to seek, the right investments in prevention and containment of risk over fines. This investment in reliability has led to low recidivism rates (See lower right, under “Results” on the Ten-Year Anniversary Placemat).

We helped to shape the move towards a more rational compliance monitoring and enforcement program, which recognizes complexity and risk. We are on the right road to becoming an adaptive, risk-informed regulator. With the help of our regional community and technical committees, our outreach efforts continue to provide clarity around shared expectations. MRO’s Standard Application Guides and our conferences and webinars are hitting the mark.

There is more to do. How do we continue to promote regional reliability? I want to highlight two areas that need more work.

Oversight. As we continue to support our reliability community, we are moving from an “audit” centric oversight approach to an integrated, comprehensive oversight approach. We need to incorporate your internal oversight program into an overall oversight plan. That’s why we work together on three-year oversight plans. You all have internal controls to do this and have had them for decades. The integration of your internal oversight program with our oversight will result in far superior risk management and more useful dialogues around risk. We can avoid duplications and reduce total costs by scaling oversight—using our tools more efficiently and effectively through a collaborative approach. As much as possible, our goal is to rely on your own internal practices to keep the small stuff small. It’s impossible to operate error-free in complexity. No one can afford it. But, you can keep the small stuff small, and really, that’s our collective job—preventing something small from cascading into something big. The premise of high reliability organizations.

It will take some time. Let me use self-logging as an example of our thinking. Today, self-logging is a standalone activity. In an integrated oversight approach, low-risk items would be logged subject to periodic inspection. There are no quarterly reports, no further action is required unless the periodic inspection determined the self-logs are poorly done, which would likely be a serious issue. We still have too much administrivia around self-logging because the regulatory response isn’t proportional and isn’t integrated into an overall oversight plan. We need to move the needle again.
Standards. Through our oversight processes, we have eliminated half of the requirements as being administrative, redundant, or minimal risk. You’ll see that on the Ten-Year Anniversary Placemat in the upper left corner under “Clarity.” NERC is discussing the next round of standards review with an eye towards eliminating unneeded requirements, similar to the Paragraph 81 initiative. Regional staff must be part of the team so we can share our work on oversight plan development—our insights about reliability in our Region. We have a list. It’s not just eliminating unneeded requirements, it’s also identifying gaps and figuring out how to best address those gaps.

On the CIP Standards, I feel like a pair of pants going through the dryer. Every time the pants go through the dryer, the lint screen takes some of the cloth or life out of the pants. That’s how I feel with CIP. CIP compliance and each revision of CIP Standards takes a little part of my life with every churn...just like a clothes dryer. There is too much churning. Too much anxiety. It may be that this is leading to misallocation of security investments. Time to go back to foundational principles.

Compliance needs to be a byproduct of good security. Plain and simple.

MRO has always taken a system architecture, tops down view for CIP. It’s the only way to address system risk. Technologies and threats change constantly. And we know that sometimes the CIP requirements get in the way of better security.

Therefore, we have a serious dilemma. The physical nature of the grid takes years to change, but the cyber systems nature of the grid can change instantaneously because of new threats or the introduction of new technologies. Standards as currently drafted have difficulties keeping up.

A few weeks ago, Gerry Cauley, NERC’s President and CEO, and I were kicking around an idea to put pen to paper on an initiative around the future of CIP to address key questions. How do we address the latest cybersecurity technologies through a standards and enforcement regime? Examples: virtualization and cloud applications. Can cybersecurity standards be designed to be enduring? Do we need to rethink our compliance monitoring and enforcement regime? Do we need mechanisms like waivers for new technologies that improve security, but are not compliant? You have heard these questions from me before, and that’s why I feel like the pair of pants in the dryer. Too much lint!

CIP reform is a tall order. But so was shifting our regulation around proportional responses—recognizing risk in our oversight. Our best ideas come from our stakeholders. As we meet new challenges, the best solutions are through a connected and collaborative community.

A Region provides a forum for you, as neighbors, to address common reliability issues and creates a collective state of mindfulness to solve problems—the key to high reliability. We have a strong reliability community.

Let me know what you’re thinking at dp.skaar@midwestreliability.org.
FROM THE MRO BOARD CHAIR

Dear Members and Stakeholders:

As I have before in this column, I would again like to consider operational reliability and resiliency of the bulk power system (BPS) by focusing on the much-anticipated Department of Energy (DOE) Staff Report to Energy Secretary Rick Perry on Electricity Markets and Reliability (“the Report”). The Report begins by noting that “[i]ssues confronting the BPS vary widely across regions”¹ and uses nine US Balancing Authorities as regions for “aggregating electricity data and revealing regional trends.”² The MRO region includes portions of the Central and Midwest sections.

I want to highlight areas of the Report in which MRO may be asked to address or work on in the future.

FACTORS AFFECTING GRID RESILIENCE

The Report considers factors that strengthen or fail to strengthen grid resilience and the associated costs. DOE staff concluded that “the grid [is] a national security asset.”³ Paraphrasing NERC President and CEO Gerry Cauley’s current reliability concerns, the Report lists four broad areas of concern:

- Insufficient amounts of reliability services (frequency and voltage support, ramping, etc.) due to resources prematurely retiring;
- Resource flexibility to respond to variable solar and wind generation;
- Fuel supply and delivery vulnerabilities due to higher reliance on natural gas; and
- The need for new transmission to support renewable resources located far from load centers.

To maintain and protect BPS reliability, the Report notes that NERC stresses the need to study evolving market, technology, policy, and regulatory factors, as well as to understand how they are affecting fuel supply, generation and transmission infrastructure planning, operations, and investment decisions. The Report then details the reliability challenges from the changing resource mix of variable energy resources and the retirement of conventional generation such as coal and nuclear. Traditional calculations of resource adequacy based on capacity (such as the planning reserve margin) will need to change due to emerging larger penetrations of variable generation.

Essential Reliability Services

The Report describes Essential Reliability Services (what we formally called “ancillary services” of frequency response, voltage support, and ramping), and noted the FERC Order that requires new interconnecting, non-synchronous generators, including wind generators, to provide

---

² Id.
³ Id. at p.16

(Continued on page 7)
reactive power as a condition of interconnection to the transmission system. DOE staff also mentioned the Primary Frequency response Notice of Proposed Rulemaking recommending that new large and small generators install, maintain, and operate equipment capable of providing primary frequency response as a condition of interconnection. These efforts by FERC will help assure sufficient frequency response as wind and other non-synchronous generators interconnect to the Grid. Essential Reliability Services are yet another area of change that will need to be taken into account for the reliability of the BPS, and NERC will have to reassess the impact they have on operational reliability and the NERC standards.

**Increasing Variable Energy Resources**

Other reliability areas touched on in the Report include inertia and energy storage. Thanks to technological advances in manufacturing and design of newer model wind turbines, those assets can now provide AGC, primary frequency response and synthetic inertia. Further study is needed on the changes to the grid because of increasing variable energy resources and decreasing rotating mass-based inertia. Likewise, energy storage will be critical to the grid when higher levels of variable energy resources are deployed, which will require additional balancing of energy supply and demand in real time. DOE noted that it has been investing in the development of energy storage technology for two decades and that commercial deployment of grid-level storage, including microgrids, has started.

The Report then focuses on the need of the Grid to meet higher levels of variable renewable energy resources and the challenges that grid operators face in operations, planning, transmission expansion practices and other sources of grid flexibility due to the characteristics of renewable resources.

**Gas and Electric Coordination**

The Report describes the diversity of generation resources, fuel assurance, and onsite storage and whether these factors cause a problem for grid reliability and resilience. The DOE believes that better system or fuel diversity with greater use of domestic energy sources enhances U.S. energy security, but does not always translate to system reliability. In fact, NERC’s 2017 State of Reliability Report identified “lack of fuel” among the top 10 causes of forced outages in 2014 and 2015. In addition, Gerry Cauley told the DOE that “[g]rowing reliance on natural gas continues to raise reliability concerns regarding the ability of both gas and electric infrastructures to maintain BPS reliability at acceptable levels.”

The Report noted that FERC and NERC are making significant strides to improve coordination between natural gas and the power industry, but that a significant amount of coordination remains unresolved.

**Resiliency and Emerging Risks**

Lastly, the Report addresses enhancing reliability and resilience in the future. DOE staff was asked to consider whether wholesale energy and capacity markets are adequately compensating attributes that strengthen grid resilience and the effect on grid reliability and resilience in the future. The DOE acknowledged that the industry currently prepares for a variety of potential threats, including high-impact, low-frequency events, to improve resilience and recovery through use of resource and fuel diversity, transmission planning, and wholesale market and product designs. These are some of the topics that were discussed in March of 2017 at NERC’s Reliability Leadership Summit on the challenges to operating the BPS, resiliency, and the identification and assessment of emerging risks to reliability.

**POLICY RECOMMENDATIONS**

The Report ends with various policy recommendations, including BPS resilience, promoting research and development of grid reliability and resilience tools, valuing Essential Reliability Services appropriately, and encouraging electric-gas coordination. The Report suggests that FERC and DOE study and facilitate efforts in these areas.

**MRO’S ROLE**

The revised ERO Enterprise Long-Term Strategy, Operating Plan, and 2018 Metrics that were posted for review and comment in September touch on some of these recommendations. In addition, in March of this year, NERC asked for comments from the Member Representatives Committee on
initiating special assessments in the areas of distributed energy resources, resource mix impacts, resource adequacy approaches, and changes to end-use load characteristics. In fact, NERC has already started a NERC special assessment on natural gas-electric interdependency. This is all good news and the industry has to continue its collaborative and technological efforts in order to fully address the impact renewables, fuel and resource diversity, infrastructure development, wholesale markets, and Essential Reliability Services have on reliability and resilience.

This industry has witnessed substantial and accelerating change over the last two decades, and this trend will likely continue into the foreseeable future. MRO, with the collaboration and support of its registered entities, will play an important role in shaping the future. We have a history of developing innovative solutions to complex problems. This kind of innovation will be needed to help industry develop policy metrics and tools for evaluating BPS-wide resilience and identifying the contributing factors that enhance (or hurt) resiliency. Also needed is our continued support of NERC as it works to identify emerging risks to reliability and protect the grid as a national security asset.

I look forward to working with you all on the challenges ahead.

(Continued from page 7 - From the MRO Board Chair)

**Introducing the ERO Enterprise Program Alignment Process**

*Sara Patrick, Vice President Compliance and Regulatory Affairs*

At the NERC Board of Trustees Compliance Committee (BOTCC) meeting in August, a panel of representatives from NERC, MRO, FRCC, and the Compliance and Certification Committee (CCC) presented information on the recently launched *ERO Enterprise Program Alignment Process.*

This process is intended to enhance efforts to identify, prioritize, and resolve alignment issues across the ERO Enterprise. This is a repeatable, transparent process that registered entities (or other relevant industry stakeholders) may use to report any perceived inconsistency in the approach, methods, or practices implemented and executed by the Regional Entities.

The ERO Enterprise Program Alignment Process relies on input from NERC’s oversight and monitoring, regional observations, and registered entity reporting. The program aims to strengthen the ERO Enterprise’s collaborative and transparent approach to resolving consistency issues.

During the BOTCC meeting, the panelists discussed how the implementation of the risk-based Compliance Monitoring and Enforcement Program (CMEP) and related oversight activities have promoted a greater degree of alignment in enforcement and compliance monitoring activities. As part of its oversight of the Regional Entities, NERC reviews the reasonableness of penalties and determinations, as well as alignment in various processes across the ERO Enterprise. NERC also works with the Regional Entities to develop and document guidance on enforcement and compliance monitoring processes and activities. Recent areas of increased alignment resulting from these efforts include risk determinations for individual violations, the allocation of credits in determining monetary penalties, and the assessment of a registered entity’s inherent risk.

Panelists also discussed how these areas of increased alignment will be tracked, triaged, and provide greater transparency under the ERO Enterprise Program Alignment Process. NERC will track identified issues from the various resources in a centralized repository. NERC will then triage the issues through an initial screening process to ensure the appropriateness for this process, then work with Regional Entities and the CCC to analyze each issue and determine its scope and materiality. The ERO Enterprise will develop recommendations and determine the priority of the activities taking into

---

1 This program was previously referred to as the Consistency Framework, but has been renamed to more accurately represent the scope of the efforts of the ERO Enterprise.
consideration all ERO Enterprise efforts. Finally, NERC will provide transparency in the process by posting the issue along with the recommendations/results in the Program Alignment – Issues and Recommendations Tracking document and providing status updates on its activities.

In support of the ERO Enterprise Program Alignment Process, NERC and the Regional Entities are in the process of developing a Regional Program Information document. The NERC Rules of Procedure allow some flexibility for Regional Entities when designing and implementing certain procedures allowing for some variation across the ERO in implementation of CMEP processes. These differences should not have a material impact on ERO Enterprise programs and should support the fair and reasonable treatment of registered entities.

To help registered entities understand where these differences exist and to increase overall transparency across the ERO Enterprise, The Regional Program Information document provides insight and transparency around each Regional Entity’s practices.

An important component supporting the ERO Enterprise Program Alignment Process is the transition of the Regional Consistency Reporting Tool from the Regional Entities to NERC. NERC implemented the newly branded Consistency Reporting Tool using a third-party application, EthicsPoint, which allows stakeholders to submit consistency issues—annonymously, if desired.

Additionally, NERC has established an email address entities can contact for more information: consistency@nerc.net.

MRO supports greater alignment across the ERO through capturing consistency concerns in a central repository, working collaboratively to prioritize the concerns, and providing transparency of the response and the actions taken to address the concerns.

The Future of Self-Logging
Jackson Evans, Enforcement Attorney

There has been an increased interest in the Self-Logging Program this year, and as a result, multiple new registered entities are now participating in the program. The Self-Logging Program includes a wide variety of program participants, who range from some of MRO’s largest registered entities to some of the smallest. All participants have reported benefits, including simplified compliance processes relating to recording, submitting and finalizing minimal risk noncompliance, and employees being more willing to bring issues forward. Further, MRO has implemented a streamlined application process to minimize the effort required from a registered entity during the application process. MRO has received feedback that MRO’s review process is uncomplicated and straightforward.

Today, self-logged issues are processed and publicly posted as Compliance Exceptions, which are not considered part of a registered entity’s compliance history and do not have an associated penalty. MRO’s vision is to enhance the program to allow minimal risk Self-Logged issues to be recorded, rather than publicly posted as a Compliance Exception filed with FERC and assigned a NERC Tracking ID. Under MRO’s vision, logged issues would be only sampled by NERC and FERC. Self-logged issues would continue to be periodically reviewed by MRO to be minimal risk and would be used in trend analysis, but they would not be publicly posted.

There are questions yet to be resolved for implementing this vision that will require input from registered entities, including whether minimal issues should be shared with industry for educational purposes (similar to current sharing of case notes), as well as how analysis on a region-wide, or continent-wide, basis could be done. MRO is actively working with its partners in the ERO Enterprise to move the Self-Logging Program forward; however, this can only be done in partnership with registered entities.

A clear path towards using the program as primarily a registered entity tracking tool will require having a critical mass of registered entities in the program, demonstrating they have the ability to identify, assess and correct minimal risk issues.

(Continued on page 10)
appropriately through their control environment. Through these entity actions, the ERO Enterprise can demonstrate to FERC and other applicable governmental authorities that industry is successfully self-detecting and correcting issues of noncompliance, and can bolster regulator confidence to move the program forward.

The Self-Logging Program is uniquely positioned to support effective regulation because it is based on registered entities taking greater control of their own compliance through self-detecting and self-correcting instances of non-compliance. Proponents of the Self-Logging Program hope that the success of this program will demonstrate that industry has the ability to take a stronger role to support the ERO Enterprise and industry grow into a more mature regulatory model.

If your organization would like more information on the Self-Logging Program or would like to apply, you can contact MRO at mro-self-logging@Midwestreliability.org.

Sue Clarke, VP Finance and Administration

Year-to-Date Financials
MRO’s June 30, 2017, unaudited actual expenses were within 0.2 percent of budget. Some staff resources are being utilized towards the new CMIP tool project. Currently staff is managing, but MRO is seeking to hire additional FTEs, which are included in the approved 2018 budget.

ERO 2018 Business Plan and Budget
The NERC board approved the Regional Entity business plans and budgets on August 10, 2017. The 2018 budget is sufficient for MRO to meet its delegated responsibilities.

NERC filed the NERC and eight Regional Entity budgets with FERC on August 24, 2017. FERC approval typically occurs in October or November.

Culture and Talent Management
This summer, MRO staff participated in various training opportunities, both required and developmental. These training opportunities enhance skills and knowledge, and help fulfill necessary continuing education requirements. MRO also provided in-house brown bag training for standards, cybersecurity, meeting procedures, and other technical topics that were facilitated by MRO staff SMEs.

These in-house presentations share information concerning industry-wide trends, organizational projects, and other updates within the MRO’s footprint.

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.

Questions regarding accounting or Human Resources can also be directed to Regina Davis, Accountant and HR Generalist.
CONFERENCE OVERVIEW

MRO is pleased to announce it is hosting its Fall Reliability Conference at our offices in Saint Paul, Minnesota and via a live WebEx stream. This one-day conference will focus on the potential planning and operational impacts of the emerging resource mix, and the essential reliability services that will need to be maintained for the reliable operations of the bulk power system.

AGENDA TOPICS

- **Update of NERC Essential Reliability Services** – Brian Evans-Mongeon, Chair NERC Planning Committee
- **Synthetic Inertia from Wind Turbine Generation** – Randy Voges, GE Renewable Energy
- **Modeling of New Generator Interconnections** – David Duebner, MISO
- **Integrating Renewables at Transmission Level and Study Tool Considerations** – Andrew Isaacs, Electranix
- **Industry Update, Lessons Learned and Alerts on Wind and Solar Power Inverters** – Rich Bauer, NERC
- **Geomagnetic Disturbances (GMD) and TPL-007 Standard** – Mark Olson, NERC
- **Utility Scale Solar Development and Experiences in the Upper Midwest** – Patrick Dalton, Xcel Energy
- **Mackinac HVDC Interconnection in UPPC** – Mike Marz, American Transmission Company, LLC
- **Battery Application** – Lin Franks, IPL
- **Geomagnetic Disturbances (GMD): A Utility Perspective** – Mike Steckelberg, Great River Energy

REGISTRATION

There is no fee to attend MRO’s Reliability Conference! A WebEx will be offered in addition to in-person attendance. You may Register [here](#). The registration deadline is October 18, 2017.

LODGING

A block of rooms has been reserved at the [Hampton Inn and Suites](#) at a rate of $169/night. You may reserve online or call 651.224.7400 and mention the room block for Midwest Reliability Organization (MRO). While the room block deadline was September 24, 2017, check with the Hampton on room availability and price.

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.
Effectively Anticipating and Mitigating Risk

The Work of MRO’s Risk Assessment, Mitigation and Standards Team

Miggie Cramblit, Co-Editor

Last week, MRO’s Vice President of Risk Assessment and Standards, Richard Burt, and I had an opportunity to talk about MRO’s Risk Assessment, Mitigation and Standards staff and the work they do to promote MRO’s Purpose: “Strive to assure each Bulk Power System owner and operator within our region is a Highly Effective Reliability Organization.”

I hope you enjoy learning about the MRO staff we call RAM.

Richard, can you tell us a bit of your background before coming to MRO and how that has helped you here at MRO?

I worked with a medium-sized generation and transmission cooperative for about 13 years prior to joining MRO, and I was fortunate to have had the opportunity to work in a number of areas. I started doing field-level SCADA and telecommunications engineering, as well as power quality studies for customers, and then transitioned to work on the company’s new Energy Management System and its supporting infrastructure. This included the operational network and associated computer systems (load forecasting, demand response, ICCP, data historian, etc.) to support real-time transmission operations. Some of the most interesting projects I worked on were developing the company’s first state estimator model and contingency analysis solution, load forecasting studies to justify the need for the first CAPX2020 project, a telecommunications upgrade from analog to digital microwave and fiber optics, and a number of EMS upgrades. I was first exposed to the NERC world when I was assigned responsibility for implementing the NERC CIP Reliability Standards when they first came into effect, and later became responsible for the O&P Standards and the company’s overall compliance program.

When I left to join MRO, I was managing both the Energy Management System and the NERC Compliance Departments, and was the company’s primary subject matter expert for every CIP Standard as well as a number of the TOP and EOP Standards.

We’ve heard about MRO’s Three Step Approach, what’s that all about?

MRO has always divided its compliance monitoring and enforcement work into three distinct departments: Compliance; Risk Assessment and Mitigation (RAM); and Enforcement. This created natural checks and balances, allowing us to ensure that an issue that made it through the CMEP process was well-founded.

Separation allows the RAM group to work with

(Continued on page 13)

1 “CapX2020 is a joint initiative of 11 transmission-owning utilities in Minnesota, North Dakota, South Dakota and Wisconsin formed to upgrade and expand the electric transmission grid to ensure continued reliable and affordable service. The projects include four 345-kilovolt transmission lines and a 230-kilovolt line. It is the largest development of new transmission in the upper Midwest in 40 years. The projects are projected to cost nearly $2 billion and cover a distance of nearly 800 miles.” See http://www.capx2020.com/index.html.
entities proactively on compliance and risk questions to ensure there is an understanding of the intent of the standard, without compromising the independence of the audit team. This separation is particularly helpful when an entity is making infrastructure changes and would like input from MRO. We’ve seen a lot of success with this approach.

Additionally, RAM staff has answered hundreds of entity questions through our HEROs@midwestreliability.org mailbox, or through one-on-one meetings with entities for more complicated topics. This outreach has been extremely effective in providing clarity to entities on the Reliability Standards and Requirements.

Well then, can you tell us a bit more about the Risk Assessment, Mitigation and Standards group at MRO?

Our primary responsibilities are risk assessment, mitigation, and outreach. RAM develops risk assessments at both the regional and entity level and relates those risks to Reliability Standard Requirements so that our Compliance Department can develop Compliance Oversight Plans based on risk. We review all noncompliances, whether they are through an audit, self-certification, or self-report, and work with the entity collaboratively to mitigate the noncompliance, which includes future prevention. We also perform a risk determination of every noncompliance based upon the specific facts and circumstances, as well as the entity’s inherent risk, to provide MRO’s Enforcement Department with a proposed risk level (minimal, moderate, or serious) and disposition method.

In addition, we review all events on the bulk power system (BPS) from a compliance perspective, act as the liaison for the MRO Standards Committee and Security Advisory Council, and lead outreach efforts on specific Reliability Standards and Requirements, such as this year’s Low Impact CIP Workshop.

Within RAM, we also have staff responsible for registration, certification, and standards development. This includes things like maintaining an inventory of all BPS Facilities in the region, performing on-site certification reviews of Transmission Operators when they replace their Energy Management System (EMS), and staying involved in Reliability Standards projects, as well as facilitating the MRO NERC Standards Review Forum (NSRF).

The NSRF allows us and our entities an efficient way to provide input into the development of new or revised NERC Standards that will have significant impact on MRO registered entities, like CIP V5. FERC and NERC staff frequently participate in the weekly NSRF meetings.

The RAM group has found that we can also add value to Reliability Standards development efforts by providing feedback based on analysis and trends we’ve observed through our risk-based CMEP activities, such as Inherent Risk Assessments, and the understanding we have of our entities’ systems and operating environments through our collaborative risk assessment and mitigation work.

Cybersecurity is one of the most critical issues for the industry. Can you tell us a little about the staff at MRO with security and control system expertise?

MRO is really blessed to be in the Minneapolis/St. Paul area, home to two of the three largest EMS vendors in the world. There’s really a lot of SCADA and security talent here, and we’ve seen the benefit of having access to that talent. Within the RAM group, we have three engineers that focus on CIP full-time: Dave, Brian, and Bill. Dave and Bill came to us from EMS vendors where they

(Continued on page 14)
designed and installed control systems for utilities all over the world, while Brian was a SCADA and telecommunications engineer at a utility, which is similar to my background. It is really beneficial to have employees with this level of technical experience when we are working with entities on mitigation plans that involve changes to their SCADA environments. For example, just recently, we were meeting with an entity’s staff on challenges they were having with CIP compliance in the entity’s substation environment. We were able to eliminate some administrative steps that had been built into the process, but weren’t required and didn’t add to security. MRO staff provided greater clarity around the technical CIP V5 requirements, many of which don’t apply if there isn’t External Routable Connectivity (ERC) to the substation. This allowed the registered entity to simplify the process—save money without increasing risk or decreasing security.

I should also mention that MRO’s CIP audit team in our Compliance Department has a very similar structure with all of MRO’s CIP auditors having considerable EMS/SCADA and utility experience.

In addition to the SCADA/EMS background, we are lucky to have Steen Fjalstad as our Security and Mitigation Principal. Steen has a Master’s Degree in Security Technologies and leads our security outreach efforts above and beyond CIP. He works with outside agencies like DHS, E-ISAC, and the FBI to ensure we are aware of and helping entities address cyber and physical security risks. This is an area that we have really expanded upon over the last couple of years with the development of a new stakeholder group, the MRO Security Advisory Council, which is devoted to security and the continued success of our annual Security Conference.

The 2017 Security Conference “sold out,” two months ahead of the scheduled conference.

The Security Conference is this week. What’s the focus of the conference?

The theme of this year’s conference is “Addressing Tomorrow’s Threats Today,” and will include presentations like “Threat Hunting” to hear about how one entity is taking proactive security approaches to actually looking for compromises, rather than just trying to prevent them. This is something that’s been around a bit in other sectors, but is now gaining momentum in the electric sector.

We will also have industry guest speakers from Arkansas Electric Cooperative Corporation, ATC, MISO, Xcel, and Marc Sachs from the Electricity Information Sharing and Analysis Center (E-ISAC). In addition to an information-packed conference agenda, we are having a free training the day before, led by Dragos Security. Dragos is a very well-respected security firm that identified the recent CrashOverride threat. Dragos was also very involved, firsthand, in the analysis of the 2015 and 2016 Ukraine power system attacks.

Who is on the Security Advisory Council and what kind of work is the Council doing?

The Security Advisory Council (SAC) is made up of experts in physical security, cybersecurity, and control systems and exists to provide counsel to MRO staff, the board of directors, and registered entities on these technical and dynamic topics. The backgrounds of the SAC members are purposefully diverse and include security executives, SCADA engineers, and security specialists from both large and small utilities. The group has had a great inaugural year. To date they have done four outreach/training events on topics such as how to get involved in GridEx, a summary of current control systems vulnerabilities, and recommended techniques to securing SCADA systems. The response has been overwhelmingly positive, with large attendance numbers at meetings and these outreach events.

In addition to an information-packed conference agenda, we are having a free training the day before, led by Dragos Security. Dragos is a very well-respected security firm that identified the recent CrashOverride threat. Dragos was also very involved, firsthand, in the analysis of the 2015 and 2016 Ukraine power system attacks.

The day after speaking at the MRO Security Conference, Marcus Sachs of E-ISAC will facilitate a meeting with the SAC to assist them in identifying unique security risks in the MRO region, which will help inform the SAC and further necessary outreach activities to help mitigate these risks with security controls.

(Continued on page 15)
The SAC is also closely coordinating and is attracting participation from DHS, FBI, E-ISAC, ICS-CERT, state regulators, and Public Safety Canada, who all regularly attend and present at the SAC’s meetings and provide insight into resources that are available to MRO registered entities for addressing security risks.

The SAC members have also been a big help in supporting our annual Security Conference, and this year Mike Kraft (Basin Electric), Jodi Jensen (WAPA), Warren LaPlante (Allete), Steve Brown (Xcel Energy), and Steen Fjalstad (MRO) will be speaking on a panel at NERC’s GRIDSEC-CON to talk about regional security work. This year GRIDSECCON is in Saint Paul, just a few blocks from MRO’s office.

MRO has always had very strong regional representation at NERC CIPC. Marc Child from Great River Energy, a MRO registered entity, is the current chair.

Creating the SAC has allowed us to continue investing in a strong, international CIPC effort, while doing more focused work within our region. As the threats and risk to the electric grid increase, we are seeing the work and focus on security increasing as well. The SAC has hit the ground running and we’ve heard a lot of positive feedback from MRO members.

Richard, thanks for taking the time to talk about the Risk Assessment, Mitigation and Standards group at MRO. If people have questions about the topics we’ve discussed how should they reach you?

We have an email address HEROs@midwestreliability.org that registered entities can use to send questions and we are happy to be of help.

HEROs?
Highly Effective Reliability Organizations, but that’s another story!

(Continued from page 14-Effectively Anticipating and Mitigating Regional Risk)
Compliance Alone is Not a Cybersecurity Strategy

Colonel Stefanie Horvath, Minnesota Army National Guard, CISSP, CRISC; Brian Isle, Senior Fellow Adventium Labs; Senior Fellow, University of Minnesota Technological Leadership Institute; and Steen Fjalstad, MRO Security and Mitigation Principal

Introduction

Today’s elevated cybersecurity challenges demand that organizations build an effective cybersecurity strategy. Many companies base their cybersecurity strategy on compliance to large security frameworks, with the general belief that compliance will protect company networks. Unfortunately, the compliance strategy is equivalent to the Maginot Line of WWII – a bulky, static defense, easily out-maneuvered by determined, highly adaptable, cyber adversaries. To explain why companies cannot fix security problems through compliance efforts alone, this paper examines “The Good, The Bad, and The Ugly” of cybersecurity strategies when compliance alone is the strategic objective. To win today’s cybersecurity conflict, the strategic approach requires a broad, adaptable cybersecurity program led by organizational leaders who understand that security is not merely a compliance issue, and requires leadership support to be effective.

The Good

Today’s security frameworks are a robust set of concepts and terms that define standardized functions, benchmarks, and semantics to produce predictive and reliable capabilities. These security frameworks evolved from years of subject matter experts assembling best practices on a broad array of security topics from good data governance, IT recovery capabilities and risk management. Standards are necessary due to the fact that they set the floor for how organizations must implement controls. For example, before the NERC Critical Infrastructure Protection (CIP) Reliability Standards came into effect in 2008, there were some electric sector organizations that did not password protect the computers that were connecting to remote substations. Rather, the computers were only protected in a physical office, sometimes using traditional door locks to limit access. After CIP, the same computer has a more secure physical perimeter with additional logical passwords, firewalls, and more robust cyber and physical security monitoring measures in place.

Consolidating these security standards and best practices into one reference, the aggregated security controls represent extensive blueprints to build a cybersecurity program. The problems arise when translating the blueprints into an actual infrastructure.

The Bad

Security frameworks fail to consider the resources necessary to operationalize the theory. These resources include the skills and workload of personnel, project management time and the materials required to build the digital defenses and protection mechanisms. Frameworks describe what “right” looks like, but lack the details on implementation, integration and assimilation into an organization’s processes and technologies. Here are a few examples:

Excessive Size and Complexity. Security frameworks are voluminous references, often with exceptionally high-level language that lack specific integration details to quickly and easily (Continued on page 17)
implement into a company’s network. For example, SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations, SP 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information, and SP 800-144 Guidelines on Security and Privacy in Public Cloud Computing are key in the suite of NIST publications describing and assessing security and privacy controls. However, the publications combined are nearly 1,000 pages of guidelines to assimilate into an actionable cybersecurity plan. "Because of the size, complexity and evolving nature of cyber threats, there is no one-size-fits-all framework applicable to all organizations."1

Closer Look at Applying the NIST standard. Applying NIST standards is a laborious process. Each step of the Risk Management Framework Security Life Cycle process has a corresponding Special Publication offering further details and guidance. Totaling 1500 pages, reading all six Special Publications is fairly daunting. A practitioner applying Asset Management controls from the NIST Cyber Security Framework (CSF) to a typical Industry Control System requires a cumbersome process of page flipping and cross referencing to find applicable security controls. A practitioner starting at ID.AM-1 must sort through the guidance to find applicable standards in NIST SP 800-53 and SP 800-82, which in turn directs the practitioner to NIST SP 800-53. Organizations have limited personnel and time to search through multiple special publications in search of control guidance.

Keeping Pace with the Adversary. Global cyber adversaries rapidly create, adapt and distribute malware at an unprecedented rate. Frameworks are not changing at the rate necessary to mitigate the morphing cyber-attacks. As noted in How to Bounce Back from Cyber Fatigue, KPMG, “Subsequent to each headline-grabbing breach comes a barrage of finger pointing, with companies asserting compliance and regulators claiming missteps. Months later, in many cases, penalties are assessed, with companies indeed discovering procedural lapses. At the same time, regulators then enhance existing compliance standards, a tacit admission that the status quo has become insufficient to evolving hacking tactics.”

By the time a new threat or emerging technology is addressed in the standards, something newer and more advanced has come along.2

Many companies are recognizing that security frameworks represent the floor, but not the ceiling, in developing a more robust cybersecurity strategy.

Keeping Pace with Technology. Emerging technologies, such as the adoption of virtualization and the advent of cloud computing, move faster than standards. Many regulated organizations want to adopt these new technologies; however, they are not able to do so and still maintain compliance with the current regulations. Furthermore, auditors are not prepared to audit many of these new technologies. Therefore, regulated organizations are caught in a conundrum of moving forward with the fear of being noncompliant or remaining stuck in the past using older technology.

Lack of Prioritization. Frameworks fail to prioritize security controls by industry risk or known cybersecurity threats. Large frameworks create a "boil the ocean" expectation, that a small number of personnel can magically implement hundreds of security controls simultaneously. A cybersecurity strategy that attempts to implement an entire framework, instead of applying the Pareto Principle to prioritize the “vital few,” diffuses the effectiveness in securing an organization’s critical data first and could burn out their staff. In the next section, we examine the Intelligence-based Risk Assessment to help organizations prioritize limited resources in forging an effective cybersecurity strategy.

Demonstrating Compliance. Many organizations are mandated to demonstrate regulatory compliance. Demonstrating regulatory compliance is largely an administrative task that can potentially force the IT security practitioner away from what they prefer to do and need to do – the cognitive function of assessing and improving the effective-

---

1 The Security Intelligence Center, Next Steps: Beyond Response to Anticipation by Raj Chaudhary and Dave McKnight.
2 Dan Skaar, Adaptive Cybersecurity Regulation

(Continued on page 18)
ness of security controls. For example, DISA requires organizations to use eMASS, a web-based Government off-the-shelf (GOTS) system. The key entry into eMASS to achieve compliance is extensive. In order to credit one network, a security practitioner must manually address over 400 security controls, encompassing 1800 acceptance procedures. Each acceptance procedure requires manual key entry and uploading an artifact. Establishing a baseline of security controls is important. However, the administrative burden to demonstrate compliance must be considered when it takes an exorbitant amount of time away from security professionals.

**Auditors and Regulators May Impose Financial Risk to Companies.** Some public companies have listed in their Annual 10-K Reports that compliance to regulations and the fines that come with noncompliance are financial risks to the companies. While this is understandable as financial impacts to any business are a risk, it is unfortunate that the regulations and the audit function that was created to help the organization and public’s best interest is being listed as a risk.

**The Cybersecurity Strategy Centered on Compliance.** Cookie cutter security frameworks violate the “art of the possible” due to sheer size of high level, conceptual language that fails to deliver critical engineering details or prioritization of work. Demonstrating compliance to these frameworks in preparation for the auditor generates an undocumented and often overlooked work activity. Organizations are driven into the compliance corral that fails to prevent or even detect the cyber adversaries.

This is where things get ugly.

**The Ugly**

The absolute ugly is the ineffectiveness of a cybersecurity strategy based on compliance. Scores of online articles from leading security organizations and experts all converge on the theme. Regulations help in many ways, but in information security today, compliance does not prevent successful attacks – it is a failing cybersecurity strategy.

- **Example 1:** One of the biggest misconceptions about PCI DSS compliance is that PCI DSS-certified companies are secure, and even more hacker-proof, as some vendors in the industry carelessly advertise.³

- **Example 2:** “Companies that suffer massive data breaches are often compliant with applicable regulations, and Sony was no exception. This doesn't mean compliance is worthless, it means too much attention is given to the checklist of technical controls instead of the processes and decisions related to information security.”⁴

³ Christian Moldes, SANS Institute InfoSec Reading room. **Compliant but not Secure: Why PCI-Certified Companies are Being Breached,** December 7, 2015.
⁴ Christopher McClean, VP and research director at Forrester Research **5 things the Sony hack exposed**

---

(Continued from page 17-Security Corner)

Strategic Lessons from a Losing Battle

**A Historical Perspective**

The Battle of Agincourt is an historical example of an unexpected major battle loss where a smaller but highly maneuverable adversary unleashed new weapons against a larger but disjointed force with extraordinary results. Nearly 6,000 Frenchmen died on the battlefield compared to 400 Englishmen. Examining the strategic decisions of both the French and English offers insight into today’s current cyber conflict. In the Battle, heavily armored French Knights may have looked good, but by day’s end, their overly heavy armor became their personal metallic coffins. “Research has proven that the heavier French armor required twice the level of energy in battle.”

French knights moved through the swampy battlefield laboriously, the weight and engineering of the armor impeding a knight’s breathing and energy. Heavy armor was not equally effective. The armor worn by the French Knights failed to protect against the Longbow, an innovative and powerful weapon of the time, with an extended range of 400 yards. Overtaxing and ineffective, today’s small cybersecurity staffs exert tremendous energy on compliance to hefty frameworks with limited defensive protection. Compliance is not protecting companies from today’s cyber Longbow.

The lethality of the Longbow, the overly heavy armor and the impact of battlefield conditions led to the destruction of French forces. Today, security practitioners are overburdened with compliance requirements, and led by those who have not developed a cybersecurity strategy consistent with the nature of the current cyber battlefield and effectiveness of cyber weapons. “Every unnecessary detour, is a waste of power, and therefore contrary to the principles of strategy.” - Carl Von Clausewitz.
A Completed Checklist Does Not Equal Cybersecurity. The less mature the regulations and auditor, the less value derived from the checklist audits. A key understanding to this failing strategy is that compliance is backward-looking, providing assurances that what has happened in the past reduced the past risks. Auditing and reviewing processes on past events may create gaps for the rapidly morphing cyber threats that continually change. The Battle of Agincourt is a historical look at strategy failing greatly by not evolving to understand the adversary and their emerging methods and weapon systems.

Building a Cybersecurity Strategy Past the Point of Compliance

Cybersecurity threats present an unprecedented overmatch for organizations. The strategy to secure the digital domain must move past compliance to become more forward-looking, therefore allowing innovation and quick adaptation. To review the importance of strategy, we offer Canadian professor Dr. Michael D. Watkins’ description in Demystifying Strategy: The What, Who, How and Why: “A strategy is therefore about how people throughout the organization should make decisions and allocate resources in order to accomplish key objectives.” A cybersecurity strategy that drives decisions and allocates resources in order to achieve compliance is drifting away from employing resources and personnel towards more responsive, real-time cybersecurity defenses.

What the Business and Industry Leadership Can Do

This section covers recommendations to build a cybersecurity strategy based on interviews and research with leading security professionals. Developing the cybersecurity strategy starts with those who develop strategy – business and industry leadership.

Develop an Organizational Culture where Security Leads. Compliance Will Follow. “In short, remember that compliance is all too often not a path to security. Security, however, if implemented and instrumented correctly, can quite often be a path to compliance” Organizations with a security culture study the adversary and engage highly-skilled IT security practitioners to formulate effective security techniques with greater consequence. In doing so, these security-minded organizations reduce cybersecurity risk to a greater extent, fulfill compliance requirements, and most importantly keep the business-critical information flowing. Organizations with a security culture realize that compliance is only the baseline they understand the risk more intuitively and knowingly generate more critical protective functions than a narrowed compliance-based lens. The contrary to a mature security culture is captured in two quotes:

“When compliance is the sole objective of security measures it’s an indication that actual security is not on a company’s radar. When this is the case, it’s a red flag – that even if a company becomes compliant, breaches may well lie ahead.”

“Not long ago, I was working on a speech and found myself trying to come up with a phrase that encapsulates the difference between organizations that really make cybersecurity a part of their culture and those that merely pay it lip service and do the bare minimum (think ‘15 pieces of flair’).”

The following are recommendations for building a resilient, adaptive and effective security organization. This type of organization puts security first, with results that meet the needs of compliance.

---

6 Wes Miller, The Desktop Files Security vs. Compliance (Microsoft TechNet)
7 Krebs on Security, What’s Your Security Maturity Level?
**Involve Employee’s Productively in Securing the Organization.** Organizations who direct their employees towards more compliance requirements could inadvertently spawn negative ramifications in compliance fatigue and reduced efficacy. “Rather than developing a solid security program that aims to reduce the actual likelihood of successful attacks, the risk management program slides into making sure that checklists for compliance are completed and auditors are happy.”

With the dramatic shortage of IT security professionals for today’s cyber conflict, organizations do not want to lose good staff because they saddled them with excessive administrative compliance requirements. Organizational leadership should be cognizant that many aspects of compliance requirements represent a burglar-stealing precious time away from good IT professionals who could be engaged in critical skillset training or project work. Career development, critical skillset training and work/life balance are all important factors for retaining a valuable IT staff.

**Lessons from the Real World.** After years of teaching organizations risk-based security assessment, Brian Isle, Senior Fellow at the University of Minnesota Technological Leadership Institute, found that if done correctly, employees enjoy thinking about the organization’s products and assets and embrace the effort to protect them by intently reviewing potential vulnerabilities. A second observation is that the people in the organization know many of the vulnerabilities and if given the tools and framework, they are happy to explore and articulate the vulnerability to develop proper mitigating actions and measures.

Using a NIST-based risk assessment in the training sessions, the attendees were taught to develop scenarios to enable an organization’s team to explore the logistics and impact of the attack. The training was done with a cross-domain team from the organization, including management. The results were that organizations change their approach to security and created the beginnings of a security culture.

The reason the training worked is many fold. First, management reinforces that security is important by the fact the team was pulled together and management is involved. Second, the assessment process is documented so the attendees can focus on getting results, not inventing the process. The process relies on and rewards the attendee’s intuitions, observations, and knowledge about the organization. Finally, the process is done as a “learning environment,” where the identification of a security issue is not focused on attributing a failure, but a quest to develop mitigation and improving the security posture.

Organizational leadership can greatly influence the company’s cybersecurity culture by supporting the learning organization initia-

---

tives, allocating resources for training and achieving compliance through methods that generate excitement, enthusiasm and innovation.

Use a “maturity model” as a Cybersecurity Strategic Roadmap. A maturity model can be the foundation to build a viable and demonstrable information security program. Author Brian Krebs offers a valuable introduction into maturity models in his article, What’s Your Security Maturity Level. Several maturity models consolidate the best information from foundational security frameworks into digestible and actionable models that organizations can implement quickly. The additional value of a maturity model is the ability to quantitatively measure an organization’s progress toward a goal, providing a semantical base for leadership and employees to describe the goals and progress and prioritize investment toward the goal. Too often the result of a cyber-incident is a knee-jerk reaction without a long term strategy. The maturity models establish the long-term strategy to synchronize cross department activities to mature cyber defenses.

Here are a few examples of available Maturity Models:

- **Example 1: Center for Internet Security’s (CIS) Critical 20 Security Controls.** The top 20 controls started as a list of best practices created by influential cyber experts. Over time, the list was validated, matured, and formalized by the CIS. The list is highly respected and provides the practitioner a common semantical basis to discuss control status and compare progress with peers. The CIS has progressed to provide secure configurations. “The CIS Benchmarks are the only consensus-based, best-practice security configuration guides both developed and accepted by government, business, industry, and academia.”

- **Example 2: Capability Maturity Model Integration (CMMI).** Carnegie Mellon University developed the CMMI as a guide to process improvement. The CMMI has been widely applied to the software development process over the last three decades. All maturity models follow, in some form, the CMMI’s 5 Characteristics of Maturity levels. The 5 levels are: Initial, Managed, Defined, Quantitatively Managed, and Optimizing. The SANS Institute InfoSec Reading Room authored the article “Using a Capability Maturity Model to Derive Security Requirements,” which offers an excellent explanation as to why an organization would use a maturity model. A more “mature” organization is defined as one whose processes are better defined and managed. Such an organization is said to have a higher capability level than a less mature organization.10

- **Example 3: Cybersecurity Capability Maturity Model (C2M2).** The Department of Energy’s C2M2 is meant to be used by an organization to evaluate its cybersecurity capabilities consistently, to communicate its capability levels in meaningful terms, and to inform the prioritization of its cybersecurity investments.11

- **Example 4: Cybersecurity Guidance Tool (CGT).** The American Water Works Association built the CGT for industrial controls systems in the water sector. The tool generates four levels of prioritized security control recommendations in response to the characterization of the facility by selecting from a menu of use-cases. The four levels of priorities align with and are a de facto maturity model. This approach enables the non-cybersecurity expert to easily translate their plant’s current configuration to a level of security maturity.

Increase Cybersecurity and Digital Innovation Simultaneously. It is critical for any company in today’s environment to increase cybersecurity given the acceleration of Information and Communication Technologies (ICT). Vice President of Digital Engagement at Schneider Electric, Natasha Nelson, presents an insightful practitioner’s point of view in her thesis “How Companies achieve balance between technology enabled innovation and cybersecurity.”12 Her findings are useful for organizations to build a cybersecurity

---

10 Mike Phillips, SANS Institute InfoSec Reading Room, *Using a Capability Maturity Model to Derive Security Requirements*, March 2003
strategic roadmap that increases cybersecurity through regulatory compliance, while, with concerted attention, flexes to enable innovation:

- Cyber-security regulations that impose penalty and require frequent assessments help shape mature cyber-security organizations that can promptly address security issues in any new technology-enabled innovations;
- Once a certain level of maturity is achieved, in well managed organizations that can be considered as following best practices, compliance focus is replaced with security focus;
- Cyber-security regulation provides a very useful tool to security teams in the early stages, as it allows them to raise the awareness across the organization, gain support from the board of directors, implement compliance measurements and embed security into most, new innovations at an early stage; however, the long term impact of cyber-security regulations have not been examined;
- Separate innovation groups can benefit from a more pro-active approach to cyber-security to enhance their estimates of the true value creation and time to market of the new initiatives.13

**Use an Intelligence-based Risk Assessment to Drive Prioritization.** An organization’s cyber-security strategy must prioritize the “vital few” cyber defense imperatives based on intelligence. By using intelligence, and an understanding of the adversary, organizations are better able to prioritize where to focus their security to gain the most benefit. Every organization has limited resources. An intelligence-based risk assessment focuses on securing the organization’s critical assets to the best ability with available resources. This intelligence-based risk assessment informs the security investments, changes to policy and procedure, and further training of security personnel.

**What Policy Makers Can Do**

The dramatic number of cybersecurity threats, the onslaught of successful breaches, and the herculean effort to secure the digital landscape is distending the “reasonable standard” for organizations to protect their networks and data. Policy makers must develop new cybersecurity policies beyond compliance that generate synchronized protection to aid in the defense of organizations instead of just penalizing them. Here’s how policymakers can help:

**Advance Compliance Oversight to Increase Compliance Value.** To alleviate the aforementioned problems that compliance is either too generic, obsolete or too prescriptive, compliance oversight must flex to address business risk and advancing technologies.

**Risk-based Compliance vs. Checklist Compliance.** When the maturity of an organization’s security program increases, so should the regulator’s maturity and the oversight methodology. This may require regulators to offer some flexibility to the monitoring staff, such as auditors, so they may adjust their methodology to focus on risk vs. checklist items based on the regulation. The regulator may be able to identify reasonable assurance using controls that do not tie directly to the regulation, but rather, to the objective the regulation is looking to accomplish. When the regulators focus on checklist items they tend to find low-risk findings, however, when the regulators focus on risk-based objectives they tend to add value and identify items the business should consider mitigating. In 2008, the National Association of Corporate Directors, the Council of Institutional Investors, and the Business Roundtable co-developed a set of Key Agreed Principles for corporate governance intended to assist boards and shareholders in avoiding rote “box ticking” in favor of a more thoughtful and studied approach.14

**Reduce the Evidentiary Overhead for Compliance Requirements.** Compiling evidence of certain security controls (related to compliance standards) occurring is a burden to many organizations. To better manage this burden more businesses are baking evidence requirements into the security controls. For example, some compliance rules require that a policy is reviewed on a periodic basis. The problem is that some businesses may not maintain evidence of a review taking place and may only review the document during a meeting and then “check-the-box.” Checking a box on a form is not ade-

---


quate evidence of a review taking place. Therefore, the process for doing the review may be better accomplished by sending an email with the file to the reviewer, and then having the reviewer electronically mark-up and sign the document they reviewed, and then email the review synopsis to a central compliance department email. The email will serve as evidence to satisfy compliance and will stand alone. This email should not require an interview of the reviewer by the regulator. For that reason, when designing security processes and controls, it is most efficient to design them to include the evidence artifacts that will also be used for compliance.

Reduce the Negative Ramifications of a Compliance Failure. The goal of compliance monitoring needs to focus on improving the security system. However, most often the results are used to punish the individual or organization. This results in a focus on successfully passing the audit rather than improving the security system. The FAA Aviation Safety Reporting System (ASRS) provides an analogy and evidence that there is a better and more effective way to administer audits. Prior to 1976, the aviation industry lacked the ability to self-report aviation safety issues. Reporting issues often resulted in resume-generating events and limited the ability to gather safety-related data. Recognizing this problem, the FAA created the ASRS that enabled safety issues to be reported with focus on improving the safety procedures rather attributing failures to individuals and organizations. The result of the 40 year-old ASRS is a continuous improvement in aviation safety. Make audits more blue than red (more integrative), allowing plans of action and mitigation to resource and implement protective defenses.

Incentivize Cybersecurity Initiatives. Policymakers could align incentives to entice the use of more secure products, clean the infrastructure and distribute threat information, thereby reducing the cybersecurity burden currently placed on companies. Here are a few examples:

- **Secure By Design**: TechTarget offers an exceptional definition of Security by Design: “an approach to software and hardware development that seeks to make systems as free of vulnerabilities and impervious to attack as possible through such measures as continuous testing, authentication safeguards and adherence to best programming practices.”

- **Use of Certified Products**: Incentivize organizations who adopt “certified” products with greater cybersecurity assurance. ISA Secure is an example of an industry standards body creating a full product development lifecycle and cyber security certification for industry products and services. Underwriter’s Laboratory (UL), a global safety science organization, recently announced its new Cybersecurity Assurance Program (UL CAP). To fuel the continuous development of certified products, policies could promote the sharing of resources between national labs and academic institutions with critical infrastructure owners and vendors serving the industry.

- **Information sharing**: From MS-ISAC to ISAOs—the aim point for every organization, regardless of size, should be to have a viable, low cost (or even free) communication channel to receive the most useful actionable intelligence information to emplace immediate security controls. With additional resourcing, MS-ISACs, ISAOs and countless organizations attempting to share cybersecurity information could broadcast viable cyber technical information to better inform ongoing risk assessments.

Conclusion

Compliance alone is not a cybersecurity strategy. No single framework can address the unique environment of an organization and respond to the accelerated speed of cyber-attacks. Organizations must develop a more robust cybersecurity strategy that deliberately assesses the threat and prioritizes limited resources to protect organizational resources. Developing an effective cybersecurity strategy is a leadership obligation. Leaders should inspire and resource a security culture that engages knowledgeable staff to reduce vulnerabilities, prioritize efforts on the most critical security projects, and develop a cybersecurity model to better track work, resources and security indicators.

Policymakers must reevaluate policies to support organizations in developing better cybersecurity strategies. Organizations are forced to adhere to a compliance requirement. Compliance is no longer a viable strategy in today’s environment where individual companies face a daily onslaught of global cyber threats. Policymakers could generate more value for organizations through policies that improve auditing functions, incentivize cybersecurity efforts and support information sharing. Organizations should have a reasonable expectation to conduct business online in a secure digital environment without excessive investment.
The authors collaborated on this article as part of their panel “Compliance Alone is not a Cybersecurity Strategy” that will be presented at the 2017 Cyber Security Summit in October 2017. More information on the Cyber Security Summit may be found here: https://cybersecuritysummit.org/

COL. STEFANIE HORVATH
Colonel, Minnesota Army National Guard, CISSP, CRISC

COL Stef Horvath is currently the J-6/CIO for the MN Army National Guard. She serves as the primary staff advisor to the Adjutant General, staff, and command officials on information technology (IT), communications, and information assurance. COL Horvath has served as a signal officer for the majority of her career, responsible for data and voice communication networks and the security of those networks. COL Horvath is the co-chair for the State of MN’s Information Security Governance committee. COL Horvath has an undergraduate degree from NDSU and a Master’s in Strategic Studies from the US Army War College. She is the recipient of the Bronze Star and Meritorious Service Medal.

BRIAN ISLE
Senior Fellow, Adventium Labs; Senior Fellow, University of Minnesota Technological Leadership Institute

Mr. Isle is the co-founder and former CEO of Adventium Labs, and a Senior Fellow at Technological Leadership Institute teaching courses in information assurance and risk assessment. Brian continues his research on critical infrastructure safety and security, building on two decades of security-related experience. Brian was a key team member for the Food Protection and Defense Institute on a DHS-funded program to improve cyber security in food manufacturing. Brian supported the DOE-funded NESCOR program to improve the cyber security readiness of the next generation power grid. Brian held key roles on a DoD program focused on vulnerability assessment for force protection and a DHS program to apply advanced cyber protection technology to control systems for critical infrastructure. Brian was honored with the 2016 Visionary Leader Award by the Cyber Security Summit. Brian is on the Board of Advisers for Technological Leadership Institute and the Cyber Security Summit.

STEEN FJALSTAD
Security and Mitigation Principal, Midwest Reliability Organization

Mr. Fjalstad works for MRO as part of the Critical Infrastructure Protection team helping to secure the North American Electric Grid (‘The Grid’). Working for MRO Steen has managed, led, and supported cyber security work with numerous North American Electric Reliability Corporation (NERC) registered entities on critical infrastructure protection. Steen coordinates with industry, local, state, and federal agencies to manage outreach efforts on threats & vulnerabilities to the Grid. Steen also manages mitigation efforts with NERC registered entities. Prior to joining MRO, Steen obtained significant experience as a security, audit, risk, and project manager with a focus on securing, designing, implementing, and auditing information technology systems. Steen has served over one-hundred different organizations spanning three continents. Steen holds a Masters Degree from University of Minnesota-Twin Cities in Security Technologies and a Bachelors degree from the University of Wisconsin-Whitewater in Management Computer Systems.
“Originals: How Non-Conformists Move the World”
by Adam Grant

A good book for anyone wanting to change the status quo...

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

We first encountered Professor Adam Grant in his book *Give and Take: Why Helping Others Drives Our Success*. His second book *Originals: How Non-Conformists Move The World* (*Originals*) is for anyone wanting to change the status quo whether it’s a societal, political, or organizational change. *Originals* relies on stories to illustrate both envisioning a new paradigm and bringing it to life. His stories are far ranging from women securing the right to vote to radical changes within the CIA to a lawyer who swims in the Arctic Sea “wearing only a Speedo, a swim cap, and goggles.”

Perhaps I was mesmerized by Grant’s storytelling, or maybe I just wasn’t concentrating enough as I was reading, but I struggled as I read the book to put together a coherent summary of how non-conformists change the world. You may too. So begin the book by copying the section “Actions for Impact,” which begins at the end on page 254. It will be a convenient place to take notes to make it easier to understand the stories and easier to implement any given action because you remember the story.

For those of you who are non-conformists, you will be validated and learn new ways to bring about change. For those of you wanting to become more original, Grant says this book is for you. Grant says “[t]he hallmark of originality is rejecting the default [or status quo] and exploring whether a better option exists.”

Grant divides the book into three sections:

- Managing the risks associated with creating and giving voice to new ideas
- Implementing strategies to establish the new idea and managing emotions
- Structuring an environment where originality flourishes

Throughout the book, Grant touches on those emotions and behaviors that that can be helpful or inhibiting in bringing about change – some of which are intuitive (curiosity is helpful) and others not so intuitive (procrastination is also helpful). Many of his concepts can be readily implemented. For example: “[O]riginals must often become tempered radicals. They believe in values that depart from traditions and ideas that go against the grain, yet they learn to tone down their radicalism by presenting their beliefs and ideas in ways that are less shocking and more appealing to mainstream audiences.” This requires a thoughtful balance in presenting original ideas in such a way that they resonate with existing beliefs and yet challenge the status quo at the same time. For example, in Dr. Martin Luther King’s *I Have a Dream* speech, King employs the call between existing beliefs (all men are guaranteed certain unalienable rights) and challenging the status quo (black men too are guaranteed certain unalienable rights) multiple times throughout his speech.

I do recommend that you buy and read this book, probably more than once. It requires effort to distill Grant. After linking his stories to the Actions for Impact, take one of the six areas of actions and focus on one or two steps in that area to build your skill set as an Original.

---

1 P 210, 2 P 7
3 Grant notes that there were two verbs for procrastination in Ancient Egypt – one for laziness and the other meaning to wait for the right time.
4 P 124, 5 P 102
The cybersecurity of Industrial Control Systems (ICS) has radically transformed over the last decade, and is a topic of concern across a multitude of industries. Increased interest has resulted in greater awareness from decision-makers at all levels, additional training options for subject-matter experts, and most importantly, additional public and private funding for cybersecurity tools and staff to protect our systems.

One byproduct of cybersecurity’s rapid growth is an increase in both the quantity and quality of ICS security information being shared across industries. This year a particular report that included significant analysis, caught my attention. On August 15, the National Infrastructure Advisory Council (NIAC) released a draft report entitled Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure. This report was created in support of Presidential Executive Order 13800, to evaluate how the Federal government could assist with the cybersecurity of critical infrastructure. The report stated, “[W]e find ourselves in a pre-9/11 level cyber moment…” Many experts managing our critical infrastructure equipment would agree with that assessment. There are parallels between what is developing in the ICS security space and historically what happened leading up to major events.

The NIAC report has 11 recommendations, of those there are three that electric industry entities could take the lead on, rather than waiting for government action. Below is a short summary and analysis of these recommendations.

**Recommendation 1: Establish Separate, Secure Communications Networks**

The report recommends identifying existing, but unused or underused fiber networks, and dedicating a “secure backup communication system to enable real-time communication during a major, cross-sector cyber-attack.” This is likely the most complicated and expensive approach to provide security to control system networks. At the same time, in theory, it is one of the best ways to secure communications networks because it provides complete control of network traffic on the physical medium. However, in practice there are typically issues both during and after implementation, resulting from the assumption that fewer security tools and protocols are needed with that level of control. It is also difficult to maintain network isolation over time as systems evolve. Still, utilities with dedicated control networks via Optical Ground Wire (OPGW) or other similar medium are more secure, with all other protections being equal.

(Continued on page 27)
Implementing plans to build out these networks is a smart long-term approach to providing additional security for transporting data between geographically-separate systems.

This recommendation also brings to mind discussions in the electric utility industry regarding the architecture of control systems and networks. The underlying function of a Supervisory Control and Data Acquisition (SCADA) system is to retrieve data from field sensors and send logical controls to operate physical equipment. An attack presents considerable risk of a widespread impact when allowing centralized systems to control local equipment, and that risk requires additional systems and tools capable of restricting these controls to a minimum set of parameters. As technology evolves, new vulnerabilities and corresponding countermeasures are developed, resulting in an ever-increasing burden on SCADA system owners.

**Recommendation 2: Machine-To-Machine Information Sharing Technologies**

Another recommendation from the council is to facilitate a private-sector-led pilot of machine-to-machine information sharing technologies, including:

- Identify and evaluate state-of-the-art technologies
- Leverage, build upon, and coordinate across existing platforms
- Identify platforms, protocols, and best practices for Information Sharing and Analysis Centers (ISACs)

Multiple vendors offer machine-to-machine information sharing, and it effectively minimizes the durations that exploits are successful on networks. Unfortunately, this is not yet a mature service for ICS networks, and has the potential to affect system reliability. There is a large volume of data utilized by these technologies, which has proven difficult to quickly analyze, or provide actionable information and intelligence with a high level of confidence. Developing these systems further will require cooperation between asset owners and utility industry vendors, to develop an effective real-time information-sharing platform for the utility industry.

**Recommendation 3: Scanning Tools and Assessment Practices**

Best-in-class scanning tools are needed to allow owners and operators of critical networks to periodically scan and sanitize their systems. The council’s recommendation calls for the following:

- Develop a voluntary, cost-shared scanning and assessment program
- Establish a Center of Excellence to showcase best-in-class tools across the industry

Out of all of the recommendations, increasing the capabilities of ICS-specific scanning tools should get the highest priority. Tools are available for IT systems that regularly scan network gateways and endpoints to determine the security status and alert or take action. These systems are typically too intrusive or ineffective on ICS networks. The effort required to perform the same functionality across the entire ICS network manually is too great for most entities. As a result, the ability to detect, mitigate and defend against cyber threats is compromised, and there is an over-reliance on network devices such as firewalls. The National Security Agency (NSA) released a publicly-available tool called GRASSMARLIN that can provide some of this functionality in ICS networks by passively monitoring network traffic or importing packet capture files. This tool is useful for network discovery and cataloging ICS devices, but more active measures could be built. For example, it can also be used to identify which ICS devices are less affected by active scanning tools, and to develop additional functionality based on this data. These tools could drastically improve an organization’s insight into the cybersecurity state of their ICS system if equipment vendors would be willing to invest in more research and development on hardening their devices and increasing capabilities.

**Conclusion**

Overall, the report was a well-presented state of the industry, and hopefully prompts the Federal government to be an active participant in addressing cybersecurity threats to critical infrastructure. The recommendations, if implemented, would provide much-needed support throughout multiple sectors. However, the process could be accelerated if private entities take the lead on the recommendations addressed. As cyber-threat capabilities increase, the electric utility industry (both asset owners and vendors) must have the ability to quickly adapt and respond with the right support and direction, in order to prevent significant cyber events. The time to act is now, as stated in the report: “There is a narrow and fleeting window of opportunity before a watershed, 9/11-level cyber-attack to organize effectively and take bold action.”
Did you know that Implementation Guidance provides examples of how to comply with NERC Reliability Standards and the ERO Enterprise will provide these examples deference during compliance monitoring and enforcement program (CMEP) activities?

In November 2015, NERC posted the Compliance Guidance Policy (Policy), which provides a mechanism for industry to share examples of methods to comply with NERC Reliability Standards. The Policy provides a process for any registered entity to work with Qualified Organizations to evaluate compliance examples with industry and submit them to the ERO Enterprise for endorsement. The ERO Enterprise’s endorsement of an example indicates the ERO Enterprise recognizes the example as one of the successful ways compliance requirements can be met given the facts and circumstances that are contained in the example.

The Policy is similar to the process that MRO utilizes with industry-developed Standard Application Guides. MRO’s President and CEO, Dan Skaar, was the executive sponsor of the ERO Compliance Guidance Policy and leveraged MRO’s experience utilizing industry expertise. Since the Policy was implemented, 18 Implementation Guidances have been endorsed by the ERO Enterprise, including the Standard Application Guides for CIP-002-5.1, FAC-008-3, and TPL-001-4 developed by MRO registered entities.

Examples of Deference During CMEP Activities

During CMEP activities, where a registered entity is following an MRO or ERO Enterprise-endorsed Implementation Guidance, CMEP staff will consider the Implementation Guidance as a possible method to achieve compliance and provide deference to its use in any compliance assessment. An entity should be prepared to demonstrate its use upon request during a compliance monitoring activity by MRO or through its own internal practices.

In the rare instance that a registered entity, in good faith, relied on Implementation Guidance, but is found non-compliant with the applicable requirements, MRO will provide deference in the processing of noncompliance where a registered entity used Implementation Guidance. The entity’s reliance on the Implementation Guidance and its good faith attempt to implement the example will be considered as a significant mitigating factor in any action by MRO.

NERC has communicated to the Regional Entities how implementation guidance should be used by ERO staff through a CMEP Practice Guide, which is an ERO Enterprise communication tool that was developed under the Policy.

Implementation Guidance is designed to be helpful to registered entities to clarify requirements. MRO staff will always provide deference for good faith efforts to use Implementation Guidance to meet requirements. We are all trying to get to the same destination in the most cost effective manner and we don’t like surprises any more than you do! If you ever have any question on Implementation Guidance, just drop us an e-mail at heros@midwestreliability.org.
VEGETATION MANAGEMENT REMAINS CRITICAL TO RELIABILITY OF THE BPS
Upcoming Fourth Quarter Self-Certification

Julie Sikes, Senior Compliance Auditor

Encroachment. The word may bring back memories of the cascading outage that occurred on August 14, 2003, when lines sagging into vegetation helped trigger a massive electrical outage. It is a word that reminds us of the importance of vegetation management and to always remain diligent in implementing vegetation management programs.

The purpose of NERC Reliability Standard FAC-003-4 summarizes the importance of vegetation management, “To maintain a reliable electric transmission system by using a defense-in-depth strategy to manage vegetation located on transmission rights of way (ROW) and minimize encroachments from vegetation located adjacent to the ROW, thus preventing the risk of those vegetation-related outages that could lead to Cascading.”

MRO registered entities have not reported a vegetation outage for several years. However, in the past two months we received two reports of vegetation-related transmission outages. In response, MRO is expediting the self-certification of FAC-003-4 R6 and R7 scheduled for 2018 to the Fourth Quarter of 2017, and is expanding the self-certification to include FAC-003-4 R3 and R5.

This self-certification provides guidance to registered entities on how to verify that vegetation programs are adequate and that vegetation maintenance is occurring as scheduled. A self-certification is an effective and efficient way for you to be able to check and monitor your own compliance with guidance from MRO on what we would look at in a review, such as an audit. By your following the guidance on the steps to take in your review, MRO has the requisite information to gain assurance of the status of your compliance with FAC-003-4, just as if MRO were conducting a spot check or audit.

We have been experiencing an exceptionally warm and wet summer in parts of the MRO region. This may have prompted remarkable vegetation growth rates, and vegetation programs need to account for expected growth rates and include the actions to be taken when conditions warrant.

Registered entities will soon be receiving the self-certification notification letter and worksheet. The submittal period for the FAC-003-4 self-certification will open October 1, 2017, and close December 31, 2017. Any questions can be sent to Julie Sikes.

APPLICATION WHITELISTING
For Control System Malware Detection and Prevention

Dave Taylor, CIP Specialist

Imagine for a minute that you are in charge of developing a plan to control who can enter a top-secret military facility through the guard station. Would you provide the guard station with:

1. a list of all the people who are not allowed to enter the facility; or
2. a list of all the people who are allowed to enter the facility?

This is obviously a silly question. List 1 would contain the names of almost every resident of planet Earth, would clearly be a nightmare to create, and impossible to maintain. List 2 would be much smaller and much easier to maintain. You might be asking yourself what this question has to do with the subject of this article. In point of fact, the question is related to how much of today’s malware detection software works. Let’s define a

(Continued on page 30)
couple of terms:

- The list of all the people who are not allowed to enter the facility would be called a **blacklist**. The signature file used by a traditional malware scanner is a form of blacklist.
- The list of all the people who are allowed to enter the facility would be called a **whitelist**.

First a brief refresher on malware scanners, they typically have two components:

- The first component is an executable software program called a **malware scanner**; it reads (scans) files that reside on storage devices, and arrive via email or over the web. The scanner scans files to compare patterns in those files to a set of “signatures.” A signature is a known pattern that is found in a particular piece of malware. Typically, a malware scanner is installed during the setup process of a new computer. This component changes infrequently, so it may only be updated a few times per year.
- The second component is something called a **signature file**, **pattern file** or other similar name. This file contains signatures (patterns) that are known to exist in malware. As new malware is identified “in the wild” vendors update signature files. These updates occur quite often, sometimes daily. To maintain maximum effectiveness, signature files on individual computers should be updated as often as they are made available by a vendor.

The signature files used by traditional malware scanners are a form of blacklist. As the electric utility industry is aware, blacklists can be difficult to maintain. They require frequent updates, which in turn requires frequent testing. Also, these signature files may be imperfect; while occurrences are rare, updates have caused problems. Finally, since anti-malware vendors typically make signature updates available via the Internet and BES Cyber Systems rarely have direct access to the Internet, moving signature file updates to those systems is often burdensome.

Another problem with signature files is that anti-malware vendors cannot add a signature for new malware until that malware has been seen “in the wild.” As a result, there is a lag time between the appearance of a new virus and the signature file update that will protect against that virus. “Zero day” attacks make use of this time lag to attack systems before anti-malware signature files have been updated.

**Application Whitelisting**

Whitelists have been in use in computer systems for a long time. Aside from signature files, other examples include:

- Firewall and router rulesets typically employ both a blacklist (i.e., a “deny everything” rule) and a whitelist which explicitly describes packets which are exceptions to the “deny everything” rule and are allowed to traverse the device.
- An email spam filter also typically employs both blacklisting and whitelisting. The list of email addresses to reject (i.e., junk senders, spammers, and junk domains) is a blacklist. The list of exceptions to an email blacklist is a form of a whitelist.

This article discusses a different type of whitelisting known as **Application Whitelisting** (AWL). AWL uses a whitelist to control which software is permitted to execute on a computer system. An AWL system will consist of three components:

1. **Application Control.** This component may be part of the operating system itself, or may be an “add on.” Its job is to intercept any attempt to execute a file, whether the file is a script, an executable (.exe), a dynamically loaded library (.DLL), or any other type of executable file. Any attempt to execute a file will cause Application Control to examine the file before permitting it to execute.

2. **Whitelist.** In our simple example, the whitelist consists of a database of digital signa-
3. Whitelist Configuration Tool. This is a tool that allows the system administrator to create and manipulate the whitelist.

Let’s assume that your organization has implemented AWL. Let’s further assume that you have convinced your boss that you need a new computer. Before your IT department delivers the new system to your eager hands, an administrator uses the Whitelist Configuration Tool to build a Whitelist which contains; all the applications that you need to do your job, as well as any background software (DLLs, scripts, background applications such as a database manager, etc.).

The Whitelist Configuration Tool will be used to compute a digital signature for each application, script, etc., that you need to use, and will add those digital signatures to the whitelist. The system administrator will use the same tool to update your Whitelist whenever a new application version, or other update is installed.

Once IT has delivered your new computer, the following takes place each time you attempt to execute a file by typing a command name, clicking on an icon, an application attempts to start other software, or even when the system automatically starts applications when it is booted:

1. Application Control computes a digital signature for the file which you have asked to be executed.
2. Application Control searches for a matching digital signature entry in the Whitelist.
   - If it finds a match, it executes the file.
   - If it does not find a match, it does not allow the file to execute and will probably issue an alert to the IT department.

A virus, or rogue script that might have arrived in an email, as a macro in a spreadsheet, or on a removable storage device, will not be included in the Whitelist and will not execute. Even a modified version of something which is in the Whitelist will have a different digital signature than that stored in the Whitelist, so it too will be prevented from executing.

Advantages of AWL include:
   - It allows system administrators to strictly define what software can execute on a machine. Importantly, it prevents a user from intentionally or accidentally downloading and executing an executable file from an unapproved source.
   - It reduces the need for frequent updates of malware scanner signature files.
   - It requires much less frequent updates than blacklisting solutions, such as traditional antivirus and malware scanners. This is especially true of many of the control systems used by electric utilities, as the software suite on such systems tends to be relatively static.
   - It is effective against zero day attacks. Traditional antivirus and malware scanners are much less effective.
   - It can work alongside traditional anti-malware solutions.

AWL does have some disadvantages:
   - If configured incorrectly, AWL can make a system difficult or even impossible to use. Many AWL solutions provide an audit only or logging mode which facilitates testing of changes to a whitelist and greatly reduces the likelihood of these problems.
   - Installing new software or updates to current software requires that the whitelist be updated, which was a significant issue in earlier versions. As AWL has matured, new tools have emerged to minimize the problem.
   - There is a small performance penalty arising from the need for the Application Control component to compute digital signatures, and perform a database lookup prior to executing a command.
   - Workstations used by software developers are not good candidates for AWL, as it can prevent applications under development from being executed. However, newer AWL solutions include features to minimize this issue.

Free AWL software is available; a) AppLocker for Microsoft Windows 7, 8, and 10; b) Gatekeeper for Apple systems; and c) a number of solutions for various Linux distributions.

Some commercial UNIX systems provide built-in AWL solutions. There are also a number of commercial, add-on, AWL solutions available from both traditional and emerging security vendors.
Implementation Guidance and Technical Rationale for Standards

Over the past 10 years the Reliability Standards template has evolved from just the standard, to also include Guidelines and Technical Basis (together “GTB”). The GTB has aided stakeholders in the implementation and application of the standards by not only providing the Standard Drafting Team’s (SDT) technical basis for the requirements, but also occasionally providing example approaches to compliance.

NERC announced at the August 9, 2017 NERC Board of Trustees meeting that it had made the determination, based on input from stakeholders, to remove the GTB from existing and future Reliability Standards given that the ERO Enterprise has now implemented a Compliance Guidance Policy (see Midwest Reliability Matters November/December 2016 issue for more details on the Compliance Guidance Policy).

Information previously found in the GTB will now be provided in either Implementation Guidance or a new document called Technical Rationale.

1. Implementation Guidance: NERC staff will coordinate a review of existing GTB to ensure Compliance Guidance language is not carried forward into the new Technical Rationale for the Standard. The Compliance Guidance process will be used to document example approaches to compliance.

2. Technical Rationale: Working with NERC staff, the NERC Standards Committee (SC) leadership recently developed the Technical Rationale in Reliability Standards document in order to provide clarity regarding the rationale used to develop the standard. The Technical Rationale will be a stand-alone document focusing on the basis for the Reliability Standard and will avoid addressing guidance regarding the implementation of the standard.

Going forward, the Reliability Standard, Compliance Guidance, and Technical Rationale will all be stand-alone documents.

FERC Reconvened, Issues Final Rules to Enhance Bulk Electric System Resilience, Reliability

According to a statement by the Federal Energy Regulatory Commission (FERC), the Commission reconvened on September 20, 2017, approving two final rules and issuing a Notice of Proposed Rulemaking addressing mandatory Reliability Standards “intended to support the resilience and reliability of the nation’s bulk electric system.”

FERC Order No. 836 approves two Reliability Standards, BAL-005-1–Balancing Authority Control and FAC-001-3–Facility Interconnection Requirements. In conjunction with the approval, FERC approved the retirement of Reliability Standards BAL-005-0.2b – Automatic Generation Control, FAC-001-2 Facility Interconnection Requirements, and BAL-006-2 – Inadvertent Interchange. The anticipated effective date of the implementation of these new Reliability Standards is October 1, 2018.

BAL-005-1 only applies to Balancing Authorities (BA); Generator Operators (GOP) and Transmission Operator (TOP) have been removed from the applicability of the standard. The obligation of ensuring all loads and facilities are within the metered boundaries of a BA have been moved to FAC-001-3. The obligation of BAs to scan data at least once every six seconds remains and the systems to calculate Area Control Error (ACE) must be available 99.95% of the time. This requirement regarding the availability of the systems to calculate ACE led to the elimination of the requirement for BAs to provide adequate and reliable backup power supplies. If a BA cannot calculate its ACE for more than 30 consecutive minutes, it must notify the Reliability Coordinator within 45 minutes of its inability to calculate its ACE. BAs must have an operating process in place to identify and mitigate errors affecting the accuracy of data used in the calculation of Reporting

(Continued on page 33)
ACE and provide the operator with data quality flags. In its filing to FERC, NERC described requirements R1, R2, R4, and R5 of BAL-006-2 as, “energy accounting standards” and/or are “administrative” in nature, and should be retired.” Requirement R3 requiring common metering points was moved to BAL-005-1.

**FERC Order No. 837** approved Reliability Standards, PRC-012-2 – Remedial Action Schemes. In conjunction with the approval, FERC approved the retirement of Reliability Standards PRC-015-1 Remedial Action Scheme Data and Documentation, and PRC-016-1 – Remedial Action Scheme Misoperation as well as NERC’s request to withdraw propose Reliability Standards PRC-012-1 – Special Protection System Review Procedure, PRC-013-1 – Remedial Action Scheme Database and PRC-014-1 – Remedial Action Scheme Assessment which were pending approval at FERC. The anticipated effective date is October 1, 2020.

The purpose of PRC-012-2 is, “To ensure that Remedial Action Schemes (RAS) do not introduce unintentional or unacceptable reliability risks to the Bulk Electric System (BES).” The standard combines all effective and pending requirements from the current and pending RAS related standards into the nine requirements of the standard. PRC-012-2 applies to Reliability Coordinators (RC), Planning Coordinators (PC) and “RAS-entity[ies] – the Transmission Owner, Generator Owner or Distribution Provider that owns all or part of a RAS.”

RCs are expected to review all RAS and provide feedback to RAS entities regarding any concerns they have identified during a review of each system. The RC is also expected to maintain and update a RAS database. The PC is required to perform evaluations at least once every 5 years of each RAS in its planning area. The RAS entity is required to submit information related to each RAS to the RC and resolve concerns identified by the RC. In the event of an operation of the RAS or failed operation, the RAS entity shall perform an analysis of the operation to determine if the RAS performed as expected and was effective. Upon completion of the analysis, if necessary, the RAS entity shall develop and implement a Corrective Action Plan (CAP) to resolve any issues. Additionally, RAS entities are required to perform functional tests of each scheme.

**Using NERC’s One-Stop-Shop Standards Page on its Website**

MRO has heard from a number of registered entities that they are having difficulty finding information related to Reliability Standards on the NERC website. The best source of this information is the Standards One-Stop-Shop spreadsheet that has existed since 2015. The One-Stop-Shop includes the entire set of documents related to the development of each standard.

Every version of a Reliability Standard approved by the NERC Board of Trustees is linked to the One-Stop-Shop regardless of its status. The dates of adoption, Effective Date of the Standard and the Inactive Data are all provided. A link to each Reliability Standard’s Implementation Plan, which details the effective date based on regulatory approval (and any phased-in implementation, if applicable), is also provided. In order to gain a better understanding of the efforts and rationale for developing a Reliability Standard, the Project Page can be accessed by selecting the Reliability Standard Title. The Project Page has links to the Standard Authorization Request or SAR, comments received, responses to comments, versions of the Reliability Standard as it was developed, and links to the results of each ballot.

When an order to approve a Reliability Standard is issued by the Federal Energy Regulatory Commission (FERC), a link to the order is posted on the One-Stop-Shop. The order may address industry comments provided to FERC and often notes FERC’s expectations in the application of the Reliability Standard, as well as any potential modifications to future versions of the Reliability Standard. The Reliability Standard Auditor Worksheets (RSAW) are also linked to the One-Stop-Shop. Any additional information related to a Reliability Standard is available through the links provided in the Related Documents, Lessons Learned and Compliance Guidance columns.

The One-Stop-Shop has greatly improved the accessibility of information related to Reliability Standards and can simply be accessed by going to the NERC Standards page on their website. Although the title of the spreadsheet calls out the “U.S.,” Canadian entities may also find this information valuable as they apply the Reliability Standards.
MRO Prepares to Conduct Annual Stakeholder Survey

An Example of How Stakeholder Input Affects Change

Miggie Cramblit, Co-Editor

Every year, MRO asks its stakeholders to complete a short survey providing input on seven basic topics:

- Newsletter
- Service
- Communications
- Training and Education
- Reliability Improvement
- Leadership
- Board of Directors

The 2017 MRO Stakeholder Survey will be sent out on November 1, 2017, to be completed by November 15, 2017. Please be sure to fill out the survey; your responses are important to us and help shape what we do.

For example, in response to the training and education question, over 80 percent of our stakeholders continue to rate the opportunities provided by MRO to participate in organizational groups and workshops as “good” to “excellent.” However, respondents also express the desire for more training and remote or virtual training. We’ve worked hard on that over the last several years and today we are offering more opportunities than ever. Last year, MRO opened its new conference center with the capabilities to live stream and record conferences and events. And this year, the MRO Security Advisory Council, our newest organizational group has hosted a number of webinars including:

1. Exploring the Unknown ICS Landscape. Presented by Rober M. Lee, CEO and Founder of Dragos, Inc., this webinar was 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 (ICS) that is unrecognized by the traditional IT cybersecurity industry. Mr. Lee walked through proven methodology, and show real-world findings and conclusions of what this means in our space. See the webinar presentation.

2. GridEx IV: Benefits and Participation Levels that Match any Sized Utility. This webinar was an introduction to NERC’s biennial grid exercise, GridEx. The webinar offered guidance on utility company participation and discussed the benefits that companies received from lessons learned of past experiences. See the webinar presentation.

3. Intelligence 101: Establishing and Maturing an Effective Threat Intelligence Program. This webinar focused on how utilities can develop a security threat intelligence program and featured example use cases from Xcel Energy, which has implemented such a program. See the webinar presentation.

In addition, MRO hosts five conferences every year: Spring Reliability Conference, Security Conference, Fall Reliability Conference, CMEP Conference, and one conference on a topic of interest, such as the CIP Low Impact Workshop held in March 2017. This education helps meet our goal to provide clarity around the regulatory requirements, assurance through a risk-based approach that encourages strong self-monitoring, and results through fast and comprehensive mitigation of risk on a voluntary basis whenever possible.

(Continued on page 35)
Upcoming 2017 Training

1. Security Technical Training Session. The MRO Security Advisory Council is sponsoring a training session this week, at the MRO offices. This session, led by Ben Miller Dragos’ Director of Threat Operations, introduces key concepts and provides a framework to develop active security defenses for control systems. It will also include demonstrations of tools and tactics that can be immediately applied.

2. MRO’s Annual Security Conference. Also scheduled this week—the day following the Security Technical Training. 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.

Both the Security Technical Training Session and the Security Conference are in-person only events because of the nature of the topics—and both events are sold out. Watch for your opportunity to attend next year and register early!

There is still time to register for the last two conferences of the year

MRO is hosting a Fall Reliability Conference on October 25, 2017. This will be held at the MRO offices and via a live WebEx stream. This one-day conference will focus on the potential planning and operational impacts of the emerging resource mix, integrating renewables, and the essential reliability services that will need to be maintained for the reliable operations of the bulk power system.

MRO is hosting a CMEP Conference on November 28, 2017. This will be held at the MRO offices and via a live WebEx stream.

In addition to these conferences and webinars, there are a number of opportunities for participating and learning. For example, the NERC Standards Review Forum (NSRF) is a group of 20-35 people who meet weekly by teleconference to review and comment on NERC Standard Authorization Requests and pending new or revised standards. The NSRF meetings are open to anyone who wants to participate, currently 130 individuals subscribe to receive NSRF information and meeting notices. This forum allows stakeholders to learn about and influence draft standards. The NSRF also uses a comment request e-mail to solicit comments from our stakeholders. If you would like to be added to this list, e-mail your request to msq@midwestreliability.org.

MRO stakeholders regularly publish technical information for registered entities. For example, our Subject Matter Expert Teams have been publishing Standard Application Guides for a number of years. Recently, MRO’s Protective Relay Subcommittee published two white papers on misoperations that identify the common causes of misoperations in the MRO Region and mitigation measures. The first whitepaper was published in April 2016 and the second whitepaper was published in June 2017.

MRO also responds to individual entity questions about the application of standards via email through the HEROs@midwestreliability.org mailbox. MRO staff vets complex questions through the ERO Enterprise (NERC and the Regions collectively), which provides greater consistency in application of standards across North America. The average response time back to the submitter has been 23 days. Response times can be longer when the questions are escalated to the ERO Enterprise to ensure consistency in approach.

Training information is also published in MRO’s bi-monthly newsletter, Midwest Reliability Matters. The newsletter covers a plethora of topics ranging from compliance tips on applying specific standards, such as BAL-001-2, COM-002-1, TOP-002-2, to factors affecting credit in enforcement actions, to articles like Why I Don’t Need a Cat by Dan Skaar, President and CEO.

Anyone can subscribe to the newsletter by submitting an email to Jessica Mitchell or through the sign-up link at www.midwestreliability.org. Each newsletter has an opportunity to provide substantive feedback.

As you can see, the feedback you provide through our Annual Stakeholder Survey produces results! We look forward to seeing what you have to say in 2017!
Because of the cybersecurity theme running throughout this anniversary issue, it seemed appropriate to review the recent cyber breach that affected the credit monitoring and reporting firm, Equifax. This cyber breach is being called the worst yet, affecting the sensitive and personally identifiable information (PII) of more than 143 million Americans—that’s roughly 44 percent of the U. S. population.

Surprisingly, the number of individuals affected by this breach isn’t the primary concern of consumer watchdogs. According to the Federal Trade Commission (FTC), the breach lasted from mid-May through July, and the hackers stole more than just names, addresses, and social security numbers. They also gained access to birthdates, the names of banking and credit institutions, and in some cases, driver’s license and credit card numbers—the information that is usually used by credit and lending organizations to verify your identity before opening a new account. This is what sets the Equifax breach apart from other similar, large-scale cybersecurity breaches, like Target and Home Depot. Once PII information has been compromised, it could be used months or even years from now, making it extremely difficult, if not impossible, to track back to Equifax. Unfortunately, the ramifications of this breach will likely be felt for many years.

Given the recent string of large-scale cyber-attacks and the likelihood that your personal information has been compromised, cyber experts are advising consumers to take action now to request new credit card numbers and freeze or place fraud alerts on credit accounts. The FTC directs individuals who aren’t sure if their information was compromised, to frequently check their credit and bank accounts as well as their credit reports for fraudulent activity.

So how did the hackers gain access to Equifax’s secure information? It appears this was a relatively easy hack. The adversaries exploited a patchable vulnerability in a web application… making this event entirely preventable.

On September 14 USA TODAY reported that Equifax acknowledged “the breach was due to a vulnerability in free, open-source software (called Apache Struts), that it used to create Java web applications.” The article also states that cybersecurity professionals had alerted Equifax about the vulnerability and the appropriate fix two months before the company was hit by hackers. In a statement about the Equifax breach, the Apache Software Foundation admitted the breach was “potentially carried out by exploiting a vulnerability in the Apache Struts Web Framework,” and said it recommends that users regularly patch and update their Apache Struts platforms. The same statement quotes vice president of Apache Struts Rene Gielen as saying “Most breaches we become aware of are caused by failure to update software components that are known to be vulnerable for months or even years.”

It doesn’t appear that the root causes of the Equifax breach have been identified yet—we only know that hackers gained access to...
Equifax’s systems through a vulnerability in a web application. Equifax continues to investigate the matter, and the company is now under federal investigation by both the Federal Trade Commission and the Consumer Financial Protection Bureau. We can only hope that these investigations will be comprehensive and that any contributing factors identified will be published to help prevent a similar occurrence.

Lack of detail aside, Ira Winkler, a contributing columnist to CSO, shared lessons that businesses can learn from the Equifax breach. In his article, Winkler raises a re-ally good point: “A single point of failure should not result in a compromise of 143 million highly valuable records.” He notes that we should be asking Equifax questions like, “Why was that volume of data so readily available to a web application? What protections should have been in place to prevent such a compromise of infor-mation? What protections should have been in place with the assumption that a web application would have an inevitable vulnerability? Was there data leak prevention in place?” According to Winkler, these types of questions address not only what failed, but also what could have been put in place to prevent such an attack.

Given what we know today, this breach serves as a good reminder of the importance of strong patch management procedures and protocols.

For our industry, we have mandatory Critical Infrastructure Protection (CIP) Reliability Standards that require the implementation of a patch management process that addresses the tracking, evaluation, and installation of cybersecurity patches on applicable Cyber Assets. A key component of these CIP requirements is the development of a mitigation plan for any identified vulnerability (typically by the installation of the patch) within 35 days of the evaluation of the patch for applicability. Had Equifax been subject to similar regulation or requirements, this breach quite possibly could have been avoided.

Equifax announced on Friday, September 22 that its chief information officer and chief security officer were retiring, effective immediately. On September 26 the CEO resigned. The company’s response to the breach hasn’t exactly been princi-pled, and the firm is being widely criticized for its slow response and lack of consumer support. But that’s another article!

---

1 See also a presentation and flow chart provided at MRO’s 2015 Security Conference on Patch Management from a registered entity perspective.
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 committed to completing COPs for all RCs, TOPs, and BAs in 2017. In September, MRO will share the remaining COPs for entities scheduled to be audited in 2018. The remaining RCs, TOPS, and BAs scheduled to be audited in 2019 will receive draft COPs by year end.

Self-Certification of FAC-003-4

In the past two months, MRO has received several Self-Reports related to vegetation management, including vegetation contact concerns. As a result, the MRO Compliance Department will be issuing a Self-Certification of FAC-003-4 R3, R5, R6 and R7. On August 25, 2017, MRO notified 18 registered entities that they will be subject to this upcoming compliance monitoring activity and indicated that they will receive formal notification of the Self-Certification in the next several weeks. The submittal period for the FAC-003-4 Self-Certification will open October 1, 2017, and close December 31, 2017.

We have been experiencing an exceptionally warm and wet summer in parts of the MRO region. This may have prompted remarkable vegetation growth rates. Vegetation programs should account for expected growth rates and the actions to be taken when issues are identified. Registered entities will be asked to verify vegetation programs are adequate and that vegetation maintenance is occurring as scheduled.

2017 Compliance Audit Status

MRO is leading six Compliance Audits in 2017 and has completed three of these six as of August 31, 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

The MRO Risk Assessment and Mitigation (RAM) Department continues to answer questions from registered entities. 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.

Regional Risk Assessment

The MRO RAM and Operations Departments have begun work on the 2018 MRO Regional Risk Assessment, which will be used to develop the 2018 Performance Areas and any Regional Risk Elements deemed necessary to complement the ERO Risk Elements. The RRA forms the basis for the 2018 CMEP Implementation Plan, and this year will include input from the MRO Operating Committee, MRO Planning Committee, and MRO Security Advisory Council regarding unique reliability and security risks in the MRO region.

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 (see Figure 1). The CSI is calculated using the Risk Determination and Discovery Method.

(Continued on page 39)
for each noncompliance. 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.

**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 to or be combined with other requirements, or even other 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 standards and requirements. This allows the same risk associated with varying instances of noncompliance to be analyzed, regardless of new 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 August 31, 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 percent of the time. This, combined with the percentages of Self-Identified violations, points

(Continued from page 38)

Breakdown of all CIP versus Non-CIP Possible Instances of Noncompliance by Year Discovered and Reported to NERC as of August 31, 2017.

Compliance Exceptions

MRO processed 154 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 154 Compliance Exceptions, 105 were Self-Identified.

Status of Alleged & Confirmed Instances of Non-Compliance

Number of Violations Processed 684 63%
Number of Findings Processed 684 63%
Number of Violations Awaiting NOP 10 1%
Number of Findings Outstanding 125 11%

Noncompliance Trends
to strong compliance commitment among registered entities in the region. 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 noncompliance. 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 percent of instances of noncompliance filed with NERC, did not contest responsibility for 5 percent of cases, and neither admitted nor denied responsibility with regards to noncompliance for 1 percent of cases (see Figure 6).

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

NERC Statement on September FERC Open Meeting
Washington, D.C.—The Federal Energy Regulatory Commission (FERC) took action on several items related to reliability as they reconvened today at the first open meeting since January 2017. FERC issued two final rules on NERC standards as well as a notice of proposed rulemaking. Read more.

FERC and NERC Joint Statement on Electricity Industry Assistance to Hurricane Irma Recovery
Washington, D.C.—FERC stated in its release that Hurricane Irma response likely will be among the largest industry restoration efforts in U.S. history. Utility industry vegetation and line crews have traveled to the region in large numbers from across the country and Canada. Read more.

FERC Issues Notice Extending Non-Statutory Deadlines due to Gulf Coast Hurricanes
Washington, D.C.—Hurricane Harvey has created emergency conditions in the Gulf Coast area of the United States, and Hurricane Irma has created or is expected to create similar emergency conditions in the Southeastern United States. Read FERC’s Notice.

Testimonies of FERC Nominees Kevin McIntyre and Richard Glick
Washington, D.C.—Kevin McIntyre and Richard Glick testimony before the Senate Energy & Natural Resources Committee on their nominations to join the Federal Energy Regulatory Commission. Read both testimonies here.

DOE Staff Report to the Secretary on Electricity Markets and Reliability
Washington, D.C.—Energy Secretary Rick Perry directed his staff to develop a report including an assessment of the reliability and resilience of the electric grid and an overview of the evolution of electricity markets. Read the full report.

DOE Invests up to $50 Million to Improve Resilience and Security of Energy Infrastructure
Washington, D.C.—The Department of Energy (National Laboratories to support early stage research and development of next-generation tools and technologies to further improve the resilience of the Nation's critical energy infrastructure, including the electric grid and oil and natural gas infrastructure. Read the more.

REGIONAL NEWS

FERC OKs Rule Changes on MISO-Manitoba Hydro Trades
September 20, 2017—FERC issued seven orders Wednesday revising how MISO deals with its neighbors when incorporating power flows between the RTO and Manitoba Hydro. Read more.

State Forces Alternative Energy Power to Come From Within Michigan
September 17, 2017—Michigan regulators issue a controversial order requiring power providers to buy or produce electricity from within the state, but the companies won’t have to comply until 2022. 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.

NERC Monitoring and Situational Awareness Technical Conference
Oct 3-4—NERC’s fifth annual Monitoring and Situational Awareness Technical Conference on October 3-4, 2017 at Georgia Power in Atlanta, Georgia. The theme of this year’s conference is EMS Solution Quality with an emphasis on modeling and real time assessment. Read more and register here.

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. 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.

MRO CMEP Conference
Nov 28—Please join us for MRO’s 2017 Annual CMEP Conference! More details will be available soon on MRO’s website.

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.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
MRO held its annual employee appreciation event on August 24, 2017 at CHS Field in Saint Paul, Minnesota—home of the Saint Paul Saints, Minnesota’s minor-league baseball team. The event was well-attended and the Saints won!

Additionally, MRO’s Volunteerism Committee organized a back to school drive this fall through the Catholic Charities Programs. This program runs several local St. Paul charities such as the St. Joseph Home for Children, School Based Counseling, and Hope Street for Homeless Youth. MRO employees donated much needed supplies such as folders, pens, pencils, calculators, and glue.

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
- Sept 27-28: Security Conference and Training
- Sept 29: Security Advisory Council Meeting
- Oct 24: Planning Committee Meeting
- Oct 25: Fall Reliability Conference
- Oct 26: Operating Committee Meeting
- Oct 31: Compliance Committee Meeting
- Nov 1: Standards Committee Meeting
- Nov 28: CMEP Conference
- Nov 30: Board Meeting

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