



CLARITY | ASSURANCE | RESULTS

MIDWEST RELIABILITY MATTERS



NOV / DEC 2011

Inside this issue:

| | |
|--|----|
| From the President | 1 |
| A Porous Enterprise, Ro-land Trope | 1 |
| Important Industry News and Events | 6 |
| Operations Report | 7 |
| Cybersecurity, More than just Compliance | 8 |
| Lessons Learned | 10 |
| CMEP Report | 12 |
| Standards Report | 15 |
| Finance and HR | 15 |
| MRO Governance | 16 |
| Event Calendar | 17 |

Share your feedback!

Please let us know what information is important to you.

To submit story ideas or other suggestions for Reliability Matters, please contact [Jessie Mitchell](#) at 651-855-1733

FROM THE PRESIDENT A Focus on Cybersecurity

MRO President, Dan Skaar

October is designated as National Cybersecurity Awareness Month in the United States, and for 2011, the theme for cybersecurity month was “***Our Shared Responsibility***.” At MRO, we recognize that we lead web-based, digital lives and this certainly extends into our industry, the Energy Sector.

As many of you know, the Energy Sector is one of the eighteen critical infrastructure sectors designated by the United States government. There is a common attribute to most of the sectors identified as “critical” – the use of control systems to operate the machinery, facilities, and equipment to provide us clean water, reliable power, safe roadways, safe chemicals, etc. For MRO staff, the emphasis and “cyber job one” for the Energy Sector is to secure control systems (ex. SCADA) from inadvertent and malicious threats.

Emphasis should be placed on the “***shared responsibility***” of cybersecurity. Cyber threats are too dynamic and “rules-based” compliance can easily be compromised. A regulatory framework of establishing a “standard by threat” is not preventative or proactive. Instead, a collaborative regulatory framework where industry is expected

(and respected) to protect its assets from cyber threat. MRO staff will work diligently with regulators to improve the Critical Infrastructure Protection (CIP) standards to ensure a secure and reliable Bulk Electric System (BES).

Government too, shares in this responsibility and has an important role in securing the BES by sharing information, providing guidance, and creating a regulatory environment that promotes good cyber security through collaboration with critical infrastructure industries. At MRO, we believe that the ERO-model is the right way to establish a collaborative, yet rigorous regulatory framework—our job is to put industry to the test!

And, each Energy Sector organization has a responsibility to have a good cybersecurity program. Cybersecurity should not be pigeon-holed in the risk management office or as a budget line item – it’s too broad, too sweeping. In my opinion, good cybersecurity takes good governance and good controls. *Good governance* creates the right environment to foster greater security throughout the organization through training, approvals, awareness, change management, etc. *Good controls* constantly evaluate your risks

and vulnerabilities – finding problems before they become exploited threats. Beyond governance and controls is the “X-factor” - human intelligence - our unique ability to add common sense to see the unusual (a threat) and act upon it. This X-factor must be instilled in the fabric of the organization - a bias for action - precaution in the face of unusual behavior from electronic devices.

In closing, our shared responsibility to cyber security goes beyond compliance. Being compliant with security regulations does not equal good security; rather, compliance is a component (the result) of a good security program.

My colleague, Mark Weatherford, former Chief Security Officer for the North American Electric Reliability Corporation (NERC) recently **blogged**, “*Compliance rarely leads to good security, but good security almost always leads to compliance. While compliance is a necessary component (some would say a necessary evil) in any high-value endeavor or like security, it’s never enough to just say, ‘I’m secure.’ That is, you must follow it up with a demonstration that you are secure. That’s compliance.*” **Good advice for us all.**

Introduction

*By Miggie Cramblit, MRO
General Counsel and Director
External Affairs*

Roland Trope and I had the pleasure of serving as co-clerks for the late Associate Justice James C. Otis of the Minnesota Supreme Court.

This excellent article is adapted from one Roland presented at the EEI Fall Legal Committee in October 2011.

It focuses on how a company should approach cybersecurity, regardless of what will need to be done in order to comply with almost any sector's particular enterprise data governance laws or standards.

By Roland L. Trope, Esq.

The U.S. corporate experience with cyber attacks recently has been real, tangible, and severely damaging (many such attacks arguably state-sponsored, state command-and-controlled, and carried out for the benefit of state(s) that denied responsibility). Companies successfully attacked last year included Google, Intel, Morgan Stanley, and several dozen other firms (dubbed "Operation Aurora").

Targets struck this year included RSA – and with data stolen from it – Lockheed Martin (dubbed "Operational Shady RAT"). As MacAfee's vice president (threat research) observed, "There are only two types of companies – those that know they've been compromised, and those that don't know. If you have anything that may be valuable to a competitor, you will be targeted, and almost certainly compromised."¹

Historically, forces of Nature have posed the greatest threats to the generation, transmission, and distribution of electricity. Companies in this field have learned to assess their threats, base their designs of defenses on such

assessments, build safeguards, and trust the resulting structure. Nations, such as The Netherlands and Japan, have implemented building policies to protect land and power stations with dikes or seawalls. In Japan, thirty-foot high sea walls on its north east coast were built to protect many seacoast towns from tsunamis. No one, however, anticipated that a major offshore earthquake would cause the Japanese seacoast to sink more than three feet. This compromised the protective seawalls and now offers a lesson in misplaced trust.

Forces of Nature attack indiscriminately. Unlike cyber forces, they are not released under the command and control of a foreign state. But existing preparedness regimes and responses to forces of Nature offer a valuable model for protecting against cyber threats and attacks.

The greatest threats to U.S. electrical utility company operations are no longer natural, but cyber. Unlike Nature's intermittent threat, cyber forces strike U.S. companies in continuous, multi-pronged assaults, often morph-

ing before they are detected in order to evade established defenses. Our cyber "sea walls" are always at risk of subsiding. What makes cyber attacks even more damaging to an enterprise is their latency. There is no warning sounded (if intrusion detection is eluded), no rising water, only the often hidden destruction or misappropriation of valuable digitized information and, with it, the potential destruction of

"The greatest threats to U.S. electrical utility company operations are no longer natural, but cyber."

power-generating capacity or the crippling of an entire grid (with an even greater potential damage once the "smart grid" comes online). The potential costs could dwarf that of a major hurricane.

As the Stuxnet attack demonstrated, multiple cyber attacks can operate undetected for months within an enterprise and, if supplemented by a "man-in-the-middle" attack, they can seize control of a SCADA system and present an "all's well" picture to operators while the attack gradually causes the system to self-destruct.

(Continued on page 3)

¹ Michael Joseph Gross, *Enter the Cyber-dragon*, Vanity Fair, September 2011, accessed at <http://www.vanityfair.com/culture/features/2011/09/chinese-hacking-201109.print>.

The absence of any visible threat or of any immediate large-scale damage (another trick of Stuxnet) creates a false sense of security. The plant operator infers that the enterprise is safe and sound.²

Once the damage has occurred and the cause traced and diagnosed, additional valuable personnel resources and time must be divided between remediating the problem (without knowing if it is fully eradicated since other payloads may be concealed within the system) and “explaining” it to regulators, lawmakers, attorney generals and the public. The pressing need for controlled disclosure and accounting for what has happened (without jeopardizing the enterprise’s legal defenses) can starve the repair effort or even work counter-productively.

It is essential, therefore, to anticipate potential threats and to have established mechanisms in place (as well as to practice and stress test them in realistic scenarios) in order to sort through a chaotic and potentially enterprise-threatening situation if it occurs. The appropriate corporate personnel must be responsible for making the right decision, at the earliest moment, otherwise the enterprise will suffer from divided focuses or mistaken triages that waste precious time, resources, and risk wasting the rapidly vanishing opportunity to contain the damage.

We have early warning systems for natural disasters, and alerted, we know how to react and

recover. Most of us have little or no experience with cyber forces. Even fewer have experience with the careful steps required (and steps that must be avoided) in order to preserve and collect the forensic digital evidence of the attacks without inadvertently destroying volatile data (by powering down units) or altering the data. Moreover, cyber attacks are often not disclosed in order not to publish an enterprise’s vulnerability, to deny an adversary any damage assessment that could help it design and launch further attacks, and to gain some advantage against future attacks from other adversaries.

Unfortunately, the advent of new communications technologies and performance enhancements or cost savings (such as those promised by cloud computing) are inevitably accompanied by new cyber vulnerabilities that may impose even greater costs in damages and recovery than the benefits and savings the enterprise has gained from the new technology.

Enterprises now need to be prepared to deal with two intersecting developments. First, the proliferation of intense, successful cyber attacks that cause severe damage to an enterprise’s digital assets. As the Division of Corporate Governance of the Securities and Exchange Commission (“Corporate Governance Division”) recently observed in its October 13, 2011 issuance of guidance regarding disclosure obligations relating to cybersecurity risks and cyber incidents (“SEC Cybersecurity Guidance”):

“[R]egistrants have migrated toward increasing dependence on digital technologies to conduct their operations. As this dependence has increased, the risks to registrants associated with cybersecurity have also increased, resulting in more frequent and severe cyber incidents.”³

And second, the continued issuance of regulations and regulatory guidance that require enterprises to meet new standards for cybersecurity and fulfill disclosure and reporting obligations concerning cybersecurity and cyber attacks which enterprises have long been reluctant to disclose because of the risks of reputational damage.

Perhaps the most significant of such issuances is the SEC Cybersecurity Guidance, both for the changes it will require in public company disclosure and the influence the Guidance will likely have on the standards that any electrical utility company may come to be required to meet. Although the SEC staff acknowledged in the Guidance that “no existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents”, it asserted that “a number of disclosure requirements may impose an obligation on registrants to disclose such risks and incidents” and that “material information regarding cybersecurity risks and cyber incidents is required to be disclosed when necessary in order to make other required disclosures...not misleading.”⁴ The SEC

(Continued on page 4)

² For a discussion of Stuxnet and the risks that cyber attacks, modeled on it, now pose to SCADA systems, see Roland L. Trope and Geoffrey Schwartz, Cyber Security for SCADA Systems, essay presented at ABA Cyber-space Winter Working Meeting, January 2011.

³ Securities and Exchange Commission, Division of Corporate Governance, CF Disclosure Guidance: Topic No. 2 Cybersecurity, October 13, 2011, p. 1, accessed at <http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm>.

⁴ SEC Cybersecurity Guidance, pp. 1 and 2.

staff identified disclosures that under the new Guidance would now be appropriate for a registrant to make, which included:

- “To the extent the registrant outsources functions that have material cybersecurity risks, description of those functions and how the registrant addresses those risks [Note: this may include any outsourcing of an electrical utilities data storage and processing to a cloud computing service];
- Description of cyber incidents experienced by the registrant that are individually, or in the aggregate, material, including a description of the costs and other consequences;
- Risks related to cyber incidents that may remain undetected for an extended period; ...”⁵

Furthermore, the SEC staff added that reputational damage, loss of customers and strategic trade secrets would also need to be considered to determine if their materiality required disclosure. Observers disagree on whether the SEC Cybersecurity Guidance will improve or compound the cybersecurity challenges that companies face. As noted in the November 1, 2011 Financial Times,

“[A] policy of deliberate ignorance might be untenable in the wake of the SEC policy. If companies start to admit dire events... [however] they could face stock sell-offs by investors. ... ‘If you are a company and 90 per cent of your revenue comes from three drugs and the formulas are gone and they are being knocked off in India, what really, is your worth?’”⁶

⁵ Ibid, p. 3.

⁶ Joseph Menn, Businesses told to reveal true scale of losses, Financial Times, November 1, 2011, Special Report “Cybersecurity”, p. 2.

1. Identify High Value Information Assets.

Few companies can afford to protect all of their digital assets. Every company can afford to protect its most critical digital assets. These will necessarily include:

first, information about its cyber defenses (lose that, and all is lost); and, *second*, its most valuable systems (such as SCADA systems) and other digital-based controls and assets (fail to protect those, and continuity of electric service and the capability to recover from disruptive outages may be compromised).

These should be the top priorities.

2. Identify Potential Sources of Cyber Vulnerabilities.

We focus here on the proliferation of cyber attacks and, in particular, on the sources of vulnerabilities that such attacks probe for, discover, and exploit. Some of the most overlooked potential sources of vulnerabilities are the following:

- a) *Deploying multiple makes of portable computing devices*
- b) *Permitting computing devices, that should be dedicated to work, to be used for personal activities, especially social networking;*
- c) *Failing to train personnel effectively on avoiding the disclosure of company-related information on web sites, in e-mails, and oth-*

er electronic media;

- d) *Failing to prohibit personnel from forwarding work email to private email accounts such as Gmail and Yahoo Mail (where such email are more vulnerable and an easier target for hackers seeking corporate data);*
- e) *Permitting high priority enterprise information to be stored where it can be accessed from beyond the company’s premises (e.g., on hard drives connected to the Internet, on wireless-enabled mobile computing devices, on smartphones, iPads, and through other data-rich portable warehouses);*
- f) *Failing to impose tight restrictions on the insertion of flash media (thumb-drives) into corporate networks;*
- g) *Permitting personnel to use, for company work, cloud-based software services, such as Google Docs and Gmail; and,*
- h) *Adopting a public cloud computing service for storage and processing of sensitive and valuable company information.*

3. Recommendations.

Many of the risks summarized above can be addressed by adopting policies that bring within the enterprise’s control activities that, if left uncontrolled, will multiply its vulnerabilities. In addition, we recommend the following precautions:

(Continued on page 5)

“Few companies can afford to protect all of their digital assets. Every company can afford to protect its most critical digital assets.”

- a) *Prepare an accurate inventory of the enterprise's "critical cyber assets" and secure them; ensure such inventory includes all information concerning the enterprise's cyber security safeguards and procedures as those must be protected above all else.*
- b) *Since cyber attacks often pierce an enterprise's defenses by causing personnel to click on links or open attachments containing the destructive payload, train personnel to recognize a variety of social engineering tricks; this will reduce the probability that they will inadvertently assist a cyber attack and enable the enterprise to demonstrate, if needed, that it took cyber security seriously.*
- c) *Since cyber security breaches will occur (and probably already have), ensure that response and recovery procedures are established and practiced.*
- d) *Ensure that the steps taken upon discovery of an attack will preserve the attack data without altering it, since such data can be invaluable in tracing the source and in diagnosing the malware in order to neutralize it.*
- e) *Devote resources to containing damage from a cyber attack to the enterprise and averting its spread to other enterprises. With increased inter-connectedness of the electrical grid, there will also be increased vulnerabilities.⁷ That, in turn, increases the probability*

ity that, if an enterprise is negligent in defending against cyber attacks, it may find itself at risk of being held liable for secondary damage caused by attacks launched later by an adversary from the enterprise's own computers.

- f) *Recognize that when breaches occur, managing the explanations will depend in part on having the enterprise speak with one voice (not many in social media) and that the micro-blogging tools (such as Twitter) will need to be monitored to keep the enterprise apprised of any misinformation that may be spreading from rumor into purported facts.*
- g) ***Any change in technology within an enterprise should be preceded by a commensurate evaluation of the security risks it poses, even a seemingly incremental change can introduce substantial new, unknown vulnerabilities (e.g., the early electronic readers could not receive or send email, but the latest iterations can, thereby placing potential treasure troves of corporate information in highly vulnerable devices accessible through insecure wireless connections).***

5. Concluding Observations.

Coping with security vulnerabilities and the risk of cyber attacks will place high demands on electrical utility industry. If addressed early and rigorously, however, the vulnerabilities created by the developments we have discussed can be

managed. Some important assumptions to start with are as follows:

- All companies are under continuous cyber attack, especially those that form part of the nation's critical infrastructure.
- Almost all U.S. enterprises are porous to such attacks. The adversaries know it; it's time for every corporate enterprise to act with that awareness.
- The number and severity of enterprise vulnerabilities is increasing faster than our ability to discover them and seal them.
- Any enterprise largely dependent for its operation on complex technology must understand how that technology makes its enterprise vulnerable to attack.
- An enterprise must also understand how the activities and habits that its employees bring into the workplace may increase those vulnerabilities.
- New technologies, and particularly new communications technologies, make our corporate "sea walls" more porous.

Reducing the vulnerability of the enterprise to cyber attacks will require sustained attention if security improvements are to be retained. Security tends to lapse when not diligently reinforced.

⁸ As the GAO recently observed, "the smart grid vision and its increased reliance on IT systems and networks expose the electric grid to potential and known cybersecurity vulnerabilities associated with using such systems, which in turn increases the risk to the smooth and reliable operation of the electricity grid. ... [T]hese vulnerabilities include: ...

- increasing the use of new system and network technologies can introduce new, unknown vulnerabilities;
- interconnecting systems and networks can allow adversaries wider access and the ability to spread malicious activity; ..."

GAO, *Electricity Grid Modernization: Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed*, GAO-11-117, January 2011, accessed at <http://www.gao.gov/new.items/d11117.pdf>.

About the Author



Roland Trope is a partner in the New York City offices of the U.S. and Dutch law firm of Trope and Schramm LLP and an Adjunct Professor in the Department of Law at the U.S. Military Academy at West Point. He is the Co-Chair of the Subcommittee on Information Security for the ABA's Cyberspace Law Committee, serves on the Supervisory Board of IEEE Security & Privacy, has written more than 25 articles, and has co-authored two law books.

Mr. Trope has over 25 years of experience in cross-border legal transactions representing governments and multi-national corporate clients. Mr. Trope advises on government procurement, export controls, compliance with anti-corruption laws, cross-border tech transfers, cyberspace law and protection and licensing of intellectual property. He represents high tech companies in the U.S., Canada, Europe and Japan and advises them on cross-border mergers and acquisitions, compliance with trade regulations (e.g., export controls, defense trade controls, trade sanctions, anti-bribery and anti-money laundering), tech transfers and licensing, corporate governance, company policies for data governance, information security, privacy and online communications, and protection and exploitation of intellectual property in government contracts.

Mr. Trope earned a B.A. in Political Science from the University of Southern California. As Marshall Scholar and as a Danforth Fellow, he studied English Language and Literature at Oxford University, earning a B.A. and M.A. He earned a J.D. at Yale Law School. He clerked on the Minnesota Supreme Court, and began practicing law in New York City in 1982.

IMPORTANT INDUSTRY NEWS AND EVENTS

NERC to Host GridEx

November 15-17, 2011. The grid security exercise will test NERC's and the electricity industry's crisis response plans, and validate current readiness in response to a cyber incident. The NERC exercise, modeled after the Department of Homeland Security's Cyber Storm exercise series, will allow participants to respond to scenario events as they would in the case of a real-time incident. This will enable participants and leadership to assess, test and validate existing crisis response plans. Read [more...](#)

DHS Appoints Weatherford Cybersecurity Chief

DHS secretary Janet Napolitano appointed Mark Weatherford, most recently VP and chief security officer of the North American Electric Reliability Corporation (NERC), as the department's new deputy undersecretary for cybersecurity for the National Protection and Programs Directorate (NPPD). The DHS NPPD is in charge of reducing threats to U.S. citizens, both physical and cyber. Read [more...](#)

NERC General Counsel to Step Down in March

NERC announced on October 17, 2011, that David Cook, Senior Vice President and General Counsel plans to step down from duties in March. NERC has begun a replacement search. Read [more...](#)

WEBINAR: Establishing an Electronic Security Perimeter Where None Previously Existed

November 18, 2011 | 11:00am—12:00pm ET
This [webinar](#), hosted by NERC, will present an overview of a process that can be used to establish an Electronic Security Perimeter (ESP) where one does not currently exist. It will discuss how to determine where the ESP should be established, along with how to determine what traffic rule sets are needed for the ESP to operate properly.

WEBINAR: Protection System Misoperation Identification and Correction

December 1, 2011 | 11a.m.–1p.m. ET
This webinar will provide a high level overview of consistent protection system and relay control misoperation reporting including a NERC 2011 second quarter misoperation summary. In addition to the misoperation summary, misoperation management success stories will be presented. **Click Here for: [Webinar Registration](#)**

Related Links:

[Department of Energy](#)
[Federal Energy Regulatory Commission](#)
[North American Electric Reliability Corporation](#)

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

[Florida Reliability Coordinating Council \(FRCC\)](#)
[SERC Reliability Corporation \(SERC\)](#)
[Texas Regional Entity \(Texas RE\)](#)
[ReliabilityFirst \(RFC\)](#)
[Western Electricity Coordinating Council \(WECC\)](#)
[Southwest Power Pool Regional Entity \(SPP RE\)](#)
[Northeast Power Coordinating Council \(NPCC\)](#)

Periodic Data Collection—Expansion of webCDMS

Salva Andiappan, Manager Reliability Assessments

MRO's Operations Department is working closely with Open Access Technology International (OATI) to identify and develop enhancements to the OATI webCDMS program to perform certain periodic data collections currently done manually by MRO Operations staff. The initial efforts are directed at improving the collection of protection system mis-operations data.

The enhancement to webCDMS includes new system architecture and processes to meet the requirements for collection and verification of the data. This effort will benefit both MRO and the Registered Entities by automating the reporting and data submission process will provide the ability to review and track submittals as well as the ability to generate reports.

It is anticipated the expanded webCDMS program will be in production for the collection of the first quarter's mis-operations in 2012. Once the system is ready to go live, a webcast training session will be available to those who are responsible for submitting the Protection System Mis-operations data. Additional information about the training and schedule will be provided when it becomes available.

Event Analysis Update

Dan Schoenecker, VP Operations

There has been significant work in recent weeks related to Event Analysis (EA). The Event Analysis Working Group (EAWG) has been updating the Event Analysis Process document based on what was learned during the two field trials and the

feedback from industry. The revised EA document should be posted on NERC's website in the next week or so.

A significant change to the process is that the five categories of events to be reported are now aligned with the draft standard EOP-004-2. The process now also places more emphasis on communication and coordination between the Registered Entity and the Regional Entity related to setting the category level and the expectations for analysis and reporting of the event.

NERC will provide training to Regional Entity Event Analysis staff in the coming weeks on cause analysis methods. The purpose of the training will be to enable staff to use causal analysis techniques for system events to determine root causal and contributing factors that lead to an event, and then develop good corrective actions or recommendations. This will help Regional Entity staff better assist Registered Entities in identifying root causes and corrective actions.

In addition to the revised process, changes to the sections of the NERC Rules of Procedures (ROP) are forthcoming related to Event Analysis. At the November 2, 2011 NERC Member Representatives Committee meeting, the stakeholders were presented with proposed revisions for Section 807 (Analysis of Major Events) and Section 808 (Analysis of Off-Normal Events, Potential System Vulnerabilities, and System Performance) of the ROP. In addition, Appendix 8 of the ROP will also be revised. The proposed changes to sections 807, 808 and Appendix 8, reflect the revised EA process developed by the EAWG. All proposed changes to the ROP can be found at <http://www.nerc.com/page.php?cid=1|8|169> MRO staff expects the pro-

posed changes will be presented to the Board of Trustees in February, 2012 for approval.

The Reliability Metrics Working Group has been working on the development of an Integrated Reliability Index. This new index will integrate 3 indexes, including an event driven index:

- *Condition Driven Index* – a measure of reliability risk based on key reliability indicators
- *Standards Driven Index* – a measure of risk based on actual violations of Reliability Standards
- *Event Driven Index* – a measure of risk from major events

In order to capture data related to system events, NERC has developed a scope for a database that will collect and process event information. For more information on the Integrated Reliability Index, please refer to NERC's [white paper](#).

For more information or questions, please contact [Dan Schoenecker](#).

JUST FOR FUN!

A mathematician, a physicist, and an engineer were all given a red rubber ball and told to find the volume.

The mathematician carefully measured the diameter and evaluated a triple integral.

The physicist filled a beaker with water, put the ball in the water, and measured the total displacement.

The engineer looked up the model and serial numbers in his red-rubber-ball table.

CYBERSECURITY...

More than just Compliance with Standards

Miggie Cramblit, General Counsel and External Affairs and Jessica Mitchell, Office Manager

In 2009, the Wall Street Journal reported: “Cyber spies have penetrated the US electric grid and left behind software programs that could be used to disrupt the system, according to current and former national security experts.”¹ William J. Lynn III, U.S. Deputy Secretary of Defense, describes the current threat situation as “[a] development of extraordinary importance - cyber technologies now exist that are capable of destroying critical networks, causing physical damage, or altering the performance of key systems. In the twenty-first century, bits and bytes are as threatening as bullets and bombs.”² Considering the increasing pace and complexity of cyber threats (the number of daily cyber-attacks on critical infrastructure networks is reported to be in the thousands), protecting the U.S. Electrical Grid from cyber attacks in this changing and increasingly risky landscape is one of the energy industry’s greatest challenges.

Despite these ominous threats, guidance in the form of law, rules, regulations or standards is nonexistent or in a state of flux. Numerous cybersecurity bills³ are pending in Congress, although none are expected to pass prior to the 2012 elections. FERC has not been able to develop consensus rules regarding proposed National Institute of Standards and Technology (“NIST”) standards for

smart grid deployment. The North American Reliability Corporation (“NERC”) Board of Trustees approved Version 4 of the Critical Infrastructure Protection (“CIP”) reliability standards CIP-002-4 through CIP-009-04 in January 2011. Those rules are now pending for comment at FERC in Docket No. RM11-11-000, with a proposed effective date the first day of the eighth quarter following approval. At the same time, the NERC Standards Committee has Version 5 of the CIP Standards (revisions of CIP-002-4 through CIP-009-04 and the addition of CIP-010-1 and CIP-011-01) pending for comment until early January 2012, and has noted that Version 5 CIP standards present “significant changes to the format and substance of the standards.” When legislation ultimately passes and regulations are finally adopted, multiple federal agencies will have a role to play in cybersecurity including the Department of Homeland Security (“DHS”), the Department of Energy (“DOE”), the NERC and the FERC.

All of this clearly represents the “VUCA” world – one filled with volatility, uncertainty, complexity and ambiguity - that President Dan Skaar has discussed in various articles and presentations. Given VUCA and the real, ever-evolving cybersecurity risk -- accompanied by not knowing what the compliance law and standards will be -- how does an entity respond?

One thing is clear: security of the electric grid rests on the control systems which oversee and operate the grid. Protection of those systems will require continuous attention and vigilance. Industry and government must work together to identify threats and perform vulnerability assessments. We must also recognize that compliance with laws and mandatory regulation may not be sufficient to respond to rapidly changing cyber technology and threats.

Mr. Trope, in his article “*A Porous Enterprise*” on page 2 of this newsletter, has provided sound and practical suggestions. Here are some additional recommendations for your consideration.

- Participate at MRO and NERC in CIP related matters to understand cybersecurity risks, to gain a sense of how the CIP standards will evolve and to shape that evolution. Here subject matter experts are needed as well as risk management personnel, lawyers and senior leadership given the complexity of the issues and processes.
- Be mindful of the evolving laws and standards, because there are and will continue to be expectations for compliance. However, the ultimate



¹ <http://online.wsj.com/article/SB123914805204099085.html>

² William J Lynn, III article “The Pentagon’s Cyberstrategy, One Year Later” <http://www.foreignaffairs.com/articles/68305/william-j-lynn-iii/the-pentagons-cyberstrategy-one-year-later>, September 28, 2011.

³ Type “cebersecurity” in the search box on the Library of Congress’ website at <http://thomas.loc.gov/cgi-bin/thomas>

end game is **reliability**. Preventing, detecting and responding to cyber attacks, in two words - security and resiliency, are inseparable to overall reliability.

- Security and resiliency will take financial and human multidisciplinary resources. It will be expensive, yet the cost will be far less than the cost of responding to a successful cyber attack.
- Take advantage of experts like [Dr. Massoud Amin](#), Professor of Electrical and Computer Engineering who holds the Honeywell/H.W. Sweatt Chair in Technological Leadership, and is also the Director of the [Technological Leadership Institute](#) at the University of Minnesota in Twin Cities.
- Build connections with the DHS since it will likely have a role in defining cybersecurity standards for the electric industry. Mark Weatherford, former vice president and chief security officer at NERC, now Deputy Under Secretary for Cybersecurity for the National Protection and Programs Directorate at the DHS, brings an understanding of the industry to DHS.
- Review the existing work done to establish control frameworks around SCADA systems, in addition to the CIP standards. Frameworks and polices can be found through the SANS Institute, Sandia Labs, NIST and ISACA, either free of charge or for a nominal fee.
- Share lessons learned so we move from a reactive to a proactive approach to cybersecurity. Understandably, Registered Entities are not eager to publicize vulnerabilities, even when doing so might assist another organization thwart the same attack. Within the current regulation, we must find ways for Registered Entities to share information without repercussion and provide a secure and effective avenue to do so – this will be an ongoing initiative for

MRO staff – enforcement should not be the tail wagging the dog.

- Most importantly, secure your control systems from malicious and inadvertent threats which could compromise, corrupt, and/or disrupt your ability to see and control your facilities on the BES. Understand what weak links exist across your control systems and work to improve security with rational plans – immediate threats require immediate attention; less immediate threats should be done according to priority.

It's important to realize that the threat of a crippling cyber-attack against critical infrastructure is *very real*, and it's imperative that the industry work to develop appropriate regulations. But we cannot wait for more legislation to pass or new standards to be approved before taking action. We must work concurrently to secure the grid recognizing the difference in managing regulatory compliance risk and managing real security risk. Failure to comply with mandatory standards can result in enforcement, but failure to secure control systems can result in reputational damage and financial distress which jeopardizes an organization's ability to perform and the bulk electric system. Security breaches cause far greater damages - you don't have to look far - SONY is a good example.

MRO's 2012 initiatives are focused on building **H**ighly **E**ffective **R**eliability **O**rganizations (HEROs), and we will continue to work towards clarity on the CIP standards and providing assurance of on-going reliability -- resulting in a secure and resilient grid.



Spare Equipment Database under Development

NERC, through the Spare Equipment Database Task Force, announced the development of a [spare equipment database](#) that allows the industry to track spare long-lead time transformers.

NERC Case Notes

NERC now has 89 [Case Notes](#) posted on their website. The Case Notes are based, in whole or in part, on information contained in mitigation plans that have been accepted by Regional Entities and approved by NERC.

NERC posts webinars on their online Resource Center

NERC's [Resource Center](#) makes educational products available to Regional Entities, industry participants, and regulators that are designed to provide the industry with the basic foundations, from the NERC perspective, to improve reliability performance, as well as assist in the development of their own, internal programs.

NERC announces ERO Best Practices from Event Analysis

[ERO Best Practices](#) are publications that highlight selected registered entity practices that are recognized by NERC as unique and add significant reliability benefit. Best Practices allow other entities to leverage that information to the benefit of Bulk Power System (BPS) reliability.

For more...www.nerc.com



TIPS

and Lessons Learned (Continued from page 6)

SHARING INFORMATION...INCREASING COMPLIANCE...STRENGTHENING RELIABILITY

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

CIP-007, R3

Guidance for Security Patch Management

Sara Patrick, Vice President Enforcement

Tracking, evaluating, testing, and installing applicable operating system, firmware and/or software security patches and security upgrades can be a formidable task for Registered Entities that have properly identified covered cyber assets. To assist with these efforts, some Registered Entities are utilizing the National Institute of Standards and Technology National Vulnerability Database (NIST NVD), a database sponsored by the Department of Homeland Security National Security Division/US-CERT. NIST NVD is the U.S. government repository of standards based vulnerability management data.

MRO received a self report of noncompliance with CIP-007-3, Requirement 3 because the Registered Entity did not evaluate, test, and install a particular security patch within the 30 day time frame required by the Standard/Requirement. The Registered Entity had conducted a search of the NIST NVD for Common Vulnerabilities and Exposures (CVEs) to identify security patches or upgrades, but no results were returned for the particular software. However, there was a new security patch available that was not identified as a result of the search. The Registered Entity subsequently learned that the NIST NVD CVE summary application names are not identical to the vendor's application names regis-

tered on the cyber assets. For instance, an application name for a Java product from Oracle was "Java™ 6," whereas the NIST NVD listed a new security patch for "Java for Business 6 Update 18, 5.0 Update 23, and 1.4.2_25." In order to ensure comprehensive monitoring for security patch management, Registered Entities utilizing NIST NVD may need to modify search terms to include broad searches for applicable security patches and security upgrades. Use of product name aliases or abbreviations may be required to find all applicable CVEs. Matching hits on the NIST NVD may still require additional refinement to assure appropriate matches.

CIP-002-3, R1

Critical Asset Identification

Steen Fjalstad, CIP Audit Manager

The Midwest Reliability Organization (MRO) has conducted many audits and spot checks of NERC Standards CIP-002 over the last two years. The process MRO has used to conduct these reviews includes using definitions found in the "NERC Glossary of Terms." NERC has defined a Critical Asset as "Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System (BES)."

The NERC standards for CIP-002-3 state "Requirement 1.2 - The risk-based assessment shall consider the following assets: Requirement 1.2.1 Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard." MRO understands that Requirement 1.2.1 has to do with the issue of operability, or more specifically, the ability of the control center to perform the applicable operating function.

To show compliance with this standard, Registered Entities should describe how control centers and

backup control centers may (or may not) affect the operability of the BES. MRO staff urges Registered Entities to use a risk-based methodology that explicitly considers control centers and their impact on the operability of the BES. Please ensure that both the reliability AND operability of the BES is taken into consideration to show compliance with CIP-002-3, R1.2.1.

You may contact mco@midwestreliability.org at any time for further discussion.

Compliance Tip Leveraging Technology

Will Smith, Mgr of Stnds & Program Performance

The current state of the economy has made it difficult for some stakeholders to justify investing in new technologies that could reduce the administrative burden of demonstrating compliance with the NERC Reliability Standards, forcing stakeholders to be innovative and derive solutions from within their existing technological infrastructure.

One of the most commonly used resources in today's information driven society is email. The email exchange system (Microsoft Out-

look, IBM Lotus Notes, etc.) is a multi-functional tool for sharing information, but can also be used as an audit trail and a records management system. Leveraging the digital footprint of an email with the attachments provides a documented step-by-step record of real process and transaction flow with actionable items that were performed during a given period of time. An entity's email and document archiving capabilities are not restricted to a hosting server. The entity can store evidentiary documentation such as an email with the attachment on another server outside of

the host email exchange server.

For example, information emailed via Microsoft Outlook can be saved outside of the hosting server using "*.msg". Whereas, saving emails derived from IBM's Lotus Notes would have to be saved as a "*.pdf" via Swing PDF Converter. Regardless of the email platform being used, archiving email-based information that contains dates and attachments can be a good resource for demonstrating compliance.

Cybersecurity Awareness

Helpful Cybersecurity Tools, Recent Publications and Noteworthy Cybersecurity News

1) The National Rural Electric Cooperative Association (NRECA) has developed a set of tools that together comprise the "[Guide to Developing a Cyber Security and Risk Mitigation Plan.](#)"

2) The *United States Computer Emergency Readiness Team (US-CERT) Control Systems Security Program (CSSP)* has released Version 4.0 of its free [Cyber Security Evaluation Tool \(CSET\)](#). This new release includes new standards such as NERC CIP Revision 3. CSET 4.0 is a free desktop software tool that guides users through a high-level process to raise awareness about their CIP compliance posture.

3) GAO's July, 2011 report entitled [CYBERSECURITY -Continued Attention Needed to Protect Our Nation's Critical Infrastructure](#) discusses threats to critical infrastructure and what the government has done and still needs to do to protect it.

4) Authored by Allan A. Friedman, the paper [Policy Frameworks for Cybersecurity Risks](#) offers three observations built around a framework of risk man-

agement to help focus the discussion of cybersecurity.

5) Our friend and colleague, Dr. Massoud Amin, Professor at the University of Minnesota's and director of the University's Technological Institute, is a regular contributor to IEEE Smart Grid Newsletter. Read his article from the February 2011 issue [Guaranteeing the Security of an Increasingly Stressed Grid.](#)

6) Eliminating threats is impossible, so protecting against them without disrupting business innovation and growth is a top management issue. Read *The McKinsey Quarterly* article [Meeting the Cybersecurity Challenge.](#)

7) Tom Alrich, Honeywell, authored an article recently on [FERC's NOPR Part 1: Through the Looking Glass.](#) The article provides insight on the status and future of CIP Version 4 with the pending approval of CIP Version 5.

8) Department of Homeland Security Secretary Janet Napolitano said recently that a major computer attack

against critical U.S. infrastructure could result in a loss of life and massive economic damages. [Read more...](#)

9) Daily cybersecurity intrusions are threatening America's ability to remain the world leader in innovation, yet few are paying attention, according to co-chairman of the Congressional Cybersecurity Caucus Rep. James Langevin (D - R.I.). [Read more...](#)

10) There's a growing apprehension within government that companies that own and operate the nation's critical infrastructures aren't doing enough to ensure that appropriate cyber-security controls are in place to protect the key resources society depends on. Read Mark Weatherford's opinion on [Solving the Compliance Versus Security Conundrum.](#)

10) Cyber security: threats and opportunities: A web panel offers utility, consultant and policy perspectives. [Read more...](#)

CMEP Report

MRO Compliance Monitoring and Enforcement Program

November 2011

Annual Implementation Plan Update

Russ Mountjoy, Compliance Audit Manager

2011 Implementation Plan

Implementation of MRO's 2011 Compliance Monitoring and Enforcement Program is on schedule.

MRO continues to work on identifying and developing the framework for a more robust compliance program. MRO's key initiative is to develop a program that assists Registered Entities in developing and implementing a compliance program that identifies and documents the controls used to continuously measure performance as required by the Reliability Standards. MRO will present this initiative at the [MRO Compliance Workshop](#) on December 14, 2011. MRO staff will assist the MRO Compliance Committee, a stakeholder group, in this effort.

2012 Implementation Plan

The 2012 MRO Implementation Plan was approved by NERC on October 31, 2011 and it is available on MRO's [website](#).

The 2012 MRO Implementation Plan mirrors the 2012 [NERC Implementation Plan](#). There is a significant change from the 2011 to 2012 implementation plans as NERC and the Regional Entities (Regions)

move to defining the scope of the audit based on tiered approach and a risk-based assessment of the Registered Entity. NERC and the Regions are finalizing the criteria and tools for assessing a Registered Entity's risk to the Bulk Power System (BPS). This project is scheduled to be completed prior to January 1, 2012.

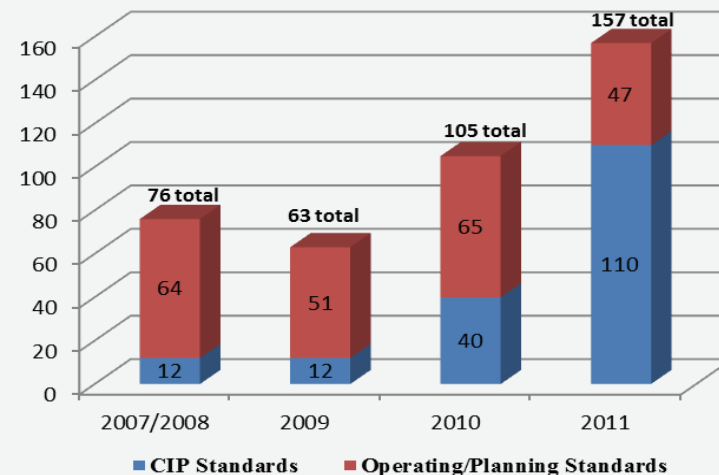
Within the MRO and NERC implementation plans, the 2012 Actively Monitored List classifies each Requirement into one of three tiers. Tier 1 requirements have been identified as the most critical requirements to the reliability of the BPS, while Tier 2 requirements tend to support Tier 1 requirements. Tier 3 requirements are those which represent the purpose of the Reliability Standard or have not been identified as a high risk standard by the ERO.

At a minimum, each audited Registered Entity will have all Tier 1 Requirements assessed during the audit process. For example, PRC-005-1, Transmission and Generation Protection System Maintenance and Testing, requirement 2 is a Tier 1 requirement which will be assessed. If the Registered Entity provides adequate evidence of maintenance and testing of its protection systems, the audit team may not need to

(Continued on page 13)

Reliability Standards Violation Statistics

Number of Possible Violations in the MRO Region Reported to NERC



Standards Most Frequently Violated (the numbers below do not include dismissals)

| Standards Most Frequently Violated | Frequency | % to Total |
|--|-----------|------------|
| PRC-005 Trans. and Gen. System Maint. and Testing | 65 | 20% |
| CIP-004 Cyber Security-Personnel and Training | 40 | 12% |
| CIP-007 Cyber Security--Systems Security Management | 37 | 12% |
| PRC-008 Implementation and Documentation of UFLS Equip Maintenance Program | 25 | 8% |
| CIP-006 Cyber Security — Physical Security of Critical Cyber Assets | 21 | 7% |
| CIP-001 Sabotage Reporting | 16 | 5% |

review R1, a Tier 2 requirement which requires having a program in place.

Based upon the risk assessment conducted by MRO staff, the scope of the audit may be increased to include Tier 2 and/or Tier 3 requirements. The risk-based assessment may take into consideration such things as past audit and spot checks, enforcement history, functions performed on the bulk electric system, reliability metrics, compliance programs and related procedures applicable to the Reliability Standards to determine the final scope of the audit. A final scope of the audit will be provided to the Registered Entity prior to the conduct of the field work and adequate time will be afforded to the Registered Entity. However, the scope of an audit can be revised depending on the facts and circumstances of the field work and MRO staff will provide Registered Entities of changes in the scope as soon as practical.

MRO staff will provide an update on risk based approaches at the upcoming December workshop.

All Registered Entities within the MRO region will be required to complete a self-certification in 2012, Registered Entities audited during the September through November 2012 timeframe will be offered the opportunity to self-certify no later than April 30, 2012.

MRO staff may determine the need for spot checks and will continue to provide the Registered Entities with sufficient notifica-

tion time. As in the past, MRO encourages Registered Entities to self-report any possible violations of Reliability Standards through webCDMS as soon as possible.

Call **Russ Mountjoy** at **651.855.1754** if you have any questions.

Annual Self-Certification Update

MRO closed the Annual Self Certification on October 28, 2011. On October 21, 2011 MRO initiated an additional Self Certification of Nuclear Generator Operators to cover two additional requirements.

Education and Training

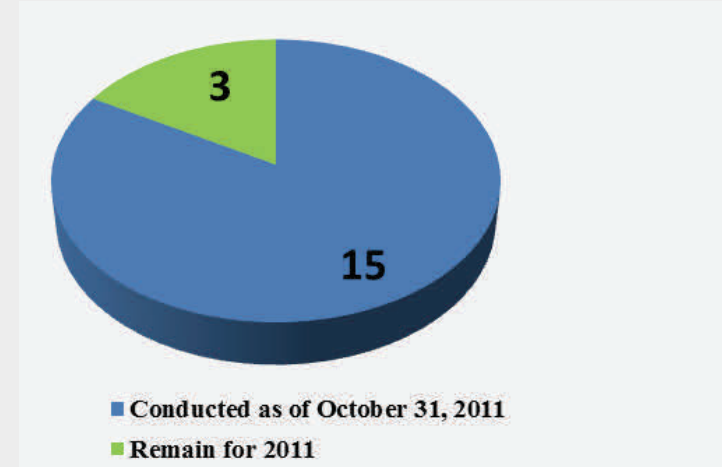
MRO is preparing the agenda for the upcoming Compliance and Enforcement Workshop that will take place on December 14, 2011 at the Crown Plaza Minneapolis (formerly known as Holiday Inn Select). More details about the workshop will be released at a later date. The workshop promises to provide new information related to the 2012 Implementation Plan as well as other important Compliance and Enforcement related items.

MRO utilizes a balanced stakeholder Standards Committee (“SC”) to educate stakeholders about the application of Reliability Standards. The SC identifies pools of Subject Matter Experts (“SME”) from industry stakeholders within the MRO region to assist in the development of application guidance for existing, new or emerging Reliability Standards.

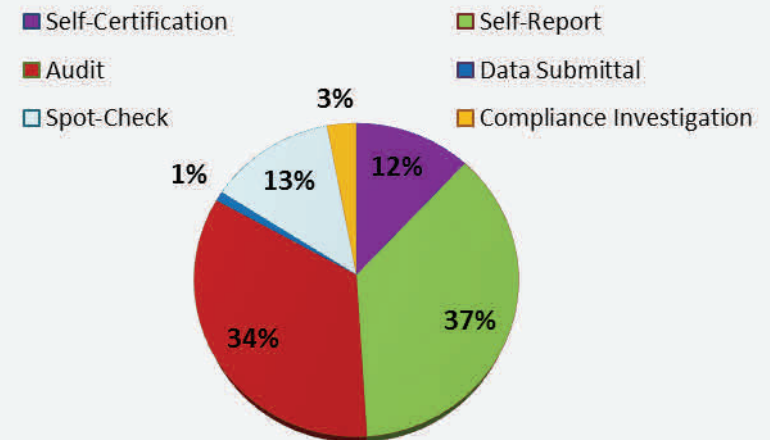
(Continued on page 14)

Compliance Audit Status

(The 2011 audit schedule can be found on MRO's [website](#))



Comparison by Discovery Method (June 18, 2007 through October 31, 2011)



**Note: Numbers above, do not include possible violations that have been dismissed*

The PER SME team is presenting application guidance for Standard PER-005 at the Mid-Continent Compliance Forum meeting on December 15, 2011.

For more information on Application Guidance, please visit the [SME web page](#) on MRO's website.

Questions?

MRO Compliance can be reached at mco@midwestreliability.org

MRO Enforcement Department can be reached at enforcement@midwestreliability.org

MRO Mitigation Department can be reached at mitigation@midwestreliability.org

{Quote of the Month}

“ We can’t solve problems by using the same kind of thinking we used when we created them”

- Albert Einstein

Comparison by Discovery Method (June 18, 2007 through October 31, 2011)

| Discovery Method Detail | June 18 - Dec 2007 | 2008 | 2009 | 2010 | 2011 YTD | Sub Total | (-less) Dismissed | Total |
|--------------------------|--------------------|-----------|-----------|------------|------------|------------|-------------------|------------|
| Self-Certification | 33 | 2 | 11 | 2 | 4 | 52 | 14 | 38 |
| Self-Report | 9 | 19 | 12 | 44 | 56 | 140 | 22 | 118 |
| Compliance Audit | 3 | 9 | 36 | 35 | 48 | 131 | 23 | 108 |
| Compliance Investigation | 0 | 0 | 0 | 0 | 10 | 10 | 1 | 9 |
| Data Submittal | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 1 |
| Spot-Check | 0 | 0 | 4 | 24 | 39 | 67 | 23 | 44 |
| Totals | 46 | 30 | 63 | 105 | 157 | 401 | 83 | 318 |

Status of Alleged and Confirmed Violations Process

| | Total ⁽¹⁾ | % |
|---|----------------------|------------|
| Total Number of Alleged Violations | 401 | 100% |
| Less: Number of Dismissals | 83 | 21% |
| Less: Number of Violations Awaiting NOP | 12 | 3% |
| Less: Number of Violations Processed ⁽²⁾ | 171 | 42% |
| Number of Violations Outstanding ⁽³⁾ | 135 | 34% |
| Total Completed | 254 | 63% |

1. Numbers are a cumulative total

2. Accepted or approved by applicable regulator, includes NOCV's, settlements, and exceptions.

3. Includes both alleged and confirmed violations yet to be processed and approved by applicable regulator (401 less 83 (Dismissed) less 171 (accepted and/or approved by regulator) less 12 (viols awaiting NOP) =135)

Status of Mitigation Plans

| Mitigation Plans | |
|---|-----|
| Number of Violations with Mitigation Plans | 202 |
| Number of Violations with Completed Mitigation Plans (validated by MRO staff) | 190 |
| Number of Violations with Outstanding Mitigation Plans to be Completed by the Registered Entity | 12 |
| Number of Late Mitigation Plans | 1 |
| Number of Violations with Mitigation Plans to be Submitted and Accepted by MRO | 116 |

FINANCE AND HUMAN RESOURCES

Year to Date Financials

MRO staff estimates that we will be slightly below budget at year end due to open staff positions. We anticipate these open positions to be filled by year end. MRO is preparing for a facility move next year, and as a result, there may be some mobilization costs incurred in 2011 which were budgeted in 2012.

2012 Business Plan and Budget

On October 20, 2011, following their Sunshine Open Meeting, the Federal Energy Regulatory Commission (FERC) issued an Order as part of Docket No. RR11-7-000 accepting the 2012 Business Plan and Budgets of NERC and the Regional Entities. MRO's

approved 2012 Business Plan and Budget can be found on MRO's website.

Culture and Talent Management

As part of our goal to bring value to those we serve through the cultivation of culture and talent, MRO continues to expand upon opportunities for employees in the areas of training and certification, E-Learning, and positive health and wellness initiatives. In addition to the corporate compliance continuing education of certified staff, MRO is preparing to launch online training programs and build a virtual training station where staff can complete required ethics and industry training. MRO is also proposing a lessons learned recap for staff in order to pro-

vide insight and future guidance when unusual circumstances call for immediate response. MRO is always seeking new ways to instruct its staff on the proper procedure and protocol for all routine and extemporaneous events.

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

Questions regarding accounts payable or receivable should be directed to [Regina Davis, Accountant and HR Specialist](#).

STANDARDS REPORT

Will Smith, Manager of Standards & Program Performance

Regional Reliability Standards

On September 22, 2011, the MRO Board of Directors approved the Standards Committee's recommendation to withdraw 4 of 5 regional standards. The four regional standards withdrawn are PRC-502-MRO-01 (Power System Stabilizer Requirement), RES-501-MRO-01 (Planned Resource Adequacy Assessment), TRL-504-MRO-01 (Subsynchronous Resonance Assessment)

and MBAL-002-0 (Operating Reserve Spinning).

The Standards Committee is currently evaluating the adequacy and effectiveness of the remaining regional standard TPL-503-MRO-02.

Application Guidance for Standard PER-005-1

The MRO Standards Committee established a team of Subject Matter Experts (SME), from Register Entities within the MRO regional footprint, to create an application

guide for NERC Reliability Standard PER-005-1 "System Personnel Training". The PER-005-1 SME team initiative is to develop non-binding guidance that identifies the necessary training to ensure competency amongst System Operators who perform reliability-related tasks on the North American Bulk Electric System.

The team is scheduled to present at the Mid-Continent Compliance Forum on December 15, 2011 at the Crowne Plaza in Bloomington, MN.

MRO GOVERNANCE - THE BOARD OF DIRECTORS

Jessica Mitchell, Assistant Corporate Secretary

Most recently, the MRO Board of Directors met in October in Winnipeg, Canada for a strategic planning session. “This meeting was one of the most productive planning sessions of the board yet,” said Dan Skaar, president of Midwest Reliability Organization, “we feel very fortunate to have a high level of professionalism and engagement from the board. Engagement from the industry is a cornerstone to meet the spirit and intent of a successful Electric Reliability Organization.” In addition to developing 2012 initiatives, changes were made to MRO’s Mission, Creed and Benchmarks of Excellence, which will be replaced by a more simple and direct *Vision, Purpose and Principles*. Both the 2012 strategic initiatives and MRO’s vision statement will be reviewed at the Annual Board and Member meeting in December for final consideration.

As reported in September, the MRO Compliance Committee (MROCC) is undertaking an initiative to create a model controls and procedures framework for use by MRO Registered Entities. To assist with this effort, the MROCC formed a new subgroup called the *Performance and Risk Oversight Subcommittee (PROS)*. On November 4, the board took action without a meeting to approve of the new subgroup and its initial roster. More information on the Compliance Committee’s initiative and the new PROS group will be provided at [MRO’s Compliance Workshop](#) on December 14, 2011.

The final board meeting of 2011 is scheduled concurrently with the *MRO Annual Member Meeting on Thursday, December 15, 2011*, at the Crowne Plaza MSP Hotel in Bloomington, MN. Board meetings are open to the public and MRO staff and the board encourage your attendance.



MRO BOARD SPOTLIGHT: MIKE RISAN

Mike Risan is the Senior Vice President of Transmission for Basin Electric Power Cooperative in Bismarck, ND. Mike began his career with Basin Electric in 1978 and had served in various capacities in the area of transmission planning when he assumed responsibility for the Transmission Department in March 2004.

Mike is a native of Parshall, North Dakota, where he graduated from high school in 1974. He earned a Bachelor of Science degree in electrical and electronics engineering with a power emphasis from North Dakota State University in 1978. He earned a masters degree in business administration from the University of North Dakota in 1996.

Mike is a registered Professional Engineer in the state of North Dakota and a Senior Member of the Institute of Electrical and Electronics Engineers (IEEE). He is a member of Eta Kappa Nu (electrical and computer engineering honor society), Tau Beta Pi (national engineering honor society), and Sigma Iota Epsilon (honorary and professional management fraternity).

Mike has been a member of the Midwest Reliability Organization Board of Directors since its inception and currently serves on the MRO Finance and Audit Committee. Mike has been active throughout his career in the activities of the Mid-Continent Area Power Pool (MAPP) and the Western Electricity Coordinating Council (WECC). Mike is also a past member of the North American Electric Reliability Corporation (NERC) Planning Committee.

Mike and his wife, Helen, have been married for 34 years and have three children: Jessica (32) and husband Dan live in Dallas, Texas with grandchildren Ellie and Bennett; Jennifer (28) is a fourth year med student at the University of North Dakota; and Jared (25) is a civil engineer. Mike and Helen enjoy spending time at their lake cabin near Detroit Lakes, Minnesota and with their kids and grandkids. Mike has also begun restoration of a 1931 Model A roadster when time permits.



Our Mission

“To be valued by those we serve as a recognized leader in promoting reliability and mitigating risks to the Bulk Power System”

CONTACT LIST

Main Phone: 651-855-1760
Main Fax: 651-855-1712
Web: www.midwestreliability.org

General & Executive

[Dan Skaar, President](#) (1731)
[Jessie Mitchell, Exec. Asst. & Office Mgr.](#) (1733)

General Counsel and External Affairs

[Miggie Cramblit, General Counsel and Director External Affairs](#) (1721)

Finance

[Sue Clarke, VP of Finance & Accounting](#) (1707)

Enforcement

[Sara Patrick, VP Enforcement and Regulatory Affairs](#) (1708)
[Jacob Phillips, Enforcement Attorney](#) (1758)
[Janice Anderson, Enforcement Admin](#) (1720)

Compliance, Mitigation and Standards

[Jim Burley, Vice President Compliance, Mitigation and Standards](#) (1748)
[Jennifer Matz, Mit & Stnd Administrator](#) (1740)
[Jo Anne McNabb, Compliance Admin](#) (1730)

Operations

[Dan Schoenecker, VP Operations](#) (1753)
[Kristine Hutchens, Operations Admin](#) (1749)
[Salva Andiappan, Mgr Reliability Assessments and Performance Analysis](#) (1719)
[John Seidel, Sr. Manager, Sit Awareness, Event Analysis and Reliability Improvement](#) (1716)

Information Technology

[Dan Schoenecker, VP Operations](#) (1753)

After Hours Emergency Line

651-734-8355

To report an MRO Region Event:
events@midwestreliability.org

EMPLOYEE NEWS

MRO is sad to announce the passing of a new, but very valuable employee, Larry Middleton. Larry was employed in the electric utility industry for more than 30 years. Prior to joining MRO, he worked as an engineering supervisor at Midwest ISO and as an Operations Engineer at American Electric Power and Mid-American Interconnected Network. Our thoughts and prayers are with Larry's family in this difficult time.

ABOUT MRO

MRO is a non-profit organization dedicated to ensuring the reliability and security of the Bulk Electric System (BES) and operates under delegated authority from regulators in both the U.S. and Canada. MRO works to develop and ensure compliance with Reliability Standards and also performs assessments of the grid's ability to meet the demands for electricity, and performs other technical analyses to improve reliability and address risks to the BPS. Additional information can be found on our website at

NOT A MEMBER YET?

MRO membership provides the following advantages:

- Participation on the various MRO committees and working groups; including the board
- Vote on key matters, such as; development of regional reliability policies and implementation
- Participate in North American and Interconnection-wide technical assessments
- Network of industry peers

MRO membership is free of charge. To apply, visit our [website](#) or call 651-855-1760

For career opportunities with MRO, please visit the [career page](#) of our website.

MRO Calendar of Events

A full meeting calendar can be found on MRO's [website](#)

| November 2011 | | | |
|---------------|--------------|--|-------------------------------------|
| Nov 15 | 9:00-12:00 | Compliance Committee | Crowne Plaza MSP Bloomington, MN |
| Nov 15 | 8:00 - 4:00 | Model Building Subcommittee | Crowne Plaza MSP Bloomington, MN |
| Nov 16 | 8:30 - 3:30 | Planning Committee Meeting | Crowne Plaza MSP Bloomington, MN |
| Nov 17 | 10:00 - 3:00 | Standards Committee Meeting | Crown Plaza MSP Bloomington, MN |
| December 2011 | | | |
| Dec 14 | 8:15 - 4:00 | MRO Compliance and Enforcement Workshop <i>(registration form)</i> | Crowne Plaza MSP Bloomington, MN |
| Dec 15 | 8:00 - 3:00 | Annual Member and Board of Directors Meeting <i>(registration form)</i> | Crowne Plaza MSP Bloomington, MN |