



MIDWEST RELIABILITY MATTERS

MAY/JUNE 2011

Special points of interest:

- FERC guidance from the recent Turlock Order (p. 2)
- Berkeley Lap Report on Reliable Integration of Variable Renewable Generation (p. 3)
- NERC releases definition of “Annual” (p. 5)
- Tracking Enforcement Actions (p. 11)
- CMEP Report (p. 13)
- Important industry updates and events (p. 16)

Inside this issue:

From the President	1
TIPS and Lessons	2
Operations Update	7
Standards Update	9
Enforcement Update	11
CMEP Report	13
Industry Updates	16
Contacts and 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**

Japan Nuclear Crisis - Lessons Learned

MRO President, Daniel P. Skaar



In the wake of the devastating natural disasters that shook Japan last month and crippled Tokyo Electric Power’s Fukushima Daiichi Nuclear Plant, one can’t help but wonder what, if *anything*, could have prevented the ensuing nuclear crisis.

A 9.0-magnitude earthquake, followed by a historic tsunami and numerous aftershocks, are extraordinary natural forces that go beyond engineering design specifications and emergency preparedness plans. One top Japanese government official was quoted as saying “The scale of the earthquake and tsunami that killed thousands and damaged the nuclear power station far surpassed what experts had planned for.”¹

The US Nuclear Regulatory Commission has been quick to disseminate lessons learned from the Japanese nuclear crisis and has launched a comprehensive review of US Nuclear Power Plant Safety. As more is learned from the specifics leading up to and following this event, long term improvements will most certainly be made.

But what can other industries, including the electric utility industry, glean from this recent disaster? The following lessons are immediately apparent:

1. Prepare. Disasters DO happen. Plan for the epic and unimaginable. Plan for cascading events.
2. Communicate. Information must be shared across state, federal and international borders, including neighboring systems. Lack of transparency undermines trust.
3. Learn. Develop lessons learned as they are instrumental to system improvements and reliability...on a broad scale.
4. Improve. Implement improvements from lessons learned -- Investments for prevention and resiliency.

Related to the latter, columnist Llewellyn King wrote an article recently for the Hearst -New York Times Syndicate defending nuclear energy.² In her article, Ms. King stressed the importance of nuclear energy to “...industrial societies [that] need large, centralized energy sources.”

Ms. King pointed out that “Titanic’s sinking in 1912 didn’t put an end to ocean liners: they got safer...Boats kept working and the technology--primarily safety valves--got better. Bad technologies are replaced by safer ones and good ones with flaws were improved upon.”

The lesson learned here is that tragedy should not define technology, but rather... *improve* it.

¹ Quote taken from Star Tribune article by Ken Belson and Andrew Pollack, April 10, 2011, found at: <http://www.startribune.com/world/119571534.html>

² Published March 21, 2011 by the Hearst-New York Times Syndicate, found at: <http://www.whchronicle.com/2011/03/nuclear-still-the-best-power-for-a-great-future/>



TIPS and Lessons Learned

SHARING INFORMATION...INCREASING COMPLIANCE...STRENGTHENING

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.

FERC Guidance from the Turlock Order FERC Orders Review of NERC Notice of Penalty for Violation of Reliability Standard

Sara E. Patrick, Director of Regulatory Affairs and Enforcement

On March 17, 2011, the Federal Energy Regulatory Commission (“FERC” or the “Commission”) issued an Order on Review of Notice of Penalty (Turlock Order) which involved a Settlement Agreement between Western Electricity Coordinating Council (WECC) and Turlock Irrigation District (Turlock). The Order affirmed the proposed \$80,000 penalty in the Settlement Agreement which included several alleged violations of NERC Reliability Standards. Notably, although there have been several instances where FERC has previously requested additional information related to Notices of Penalty, this is the first instance where FERC has undertaken review of a Notice of Penalty.

FERC initiated review of one of the alleged violations in the Notice of Penalty, FAC-003-1, R2, which requires an entity to create and implement an annual plan for vegetation management. Turlock had reported a violation of FAC-003-1 resulting from an August 29, 2007 230 kilovolt (“kV”) line outage and firm load shedding to WECC. WECC and Turlock independently concluded that Turlock failed to adequately follow its 2007 Vegetation Management Work Plan, which allowed an almond tree to grow into a 230 kV power line causing an outage to thousands.

In the Turlock Order, FERC placed significant importance on the fact that the alleged violation of FAC-003-1, R2 occurred within several weeks after the Standard became effective and mandatory in the United States. In addition to approving the proposed penalty, FERC provided guidance on several “factors that could affect future reviews.” These factors include:

– **Load Shedding.** FERC explained that while load loss alone is not a violation (and may be necessary or required by reliability standards), if load loss results from a reliability standard violation, the penalty assessed for the violation should consider the lost load because the violation created a more serious risk or result than a similar violation that did not necessitate load shedding.

- **A Registered Entity's Efforts after an Alleged Violation.** FERC stated that a Registered Entity’s effort to achieve or maintain compliance with the NERC Reliability Standards is not a basis for a reduction in a proposed penalty amount. However, if a Registered Entity undertakes “significantly enhanced efforts” in response to its violation of a NERC Reliability Standard, these above and beyond actions may be considered as an offset to a proposed penalty amount.
- **Cooperation versus Self-Reporting.** FERC clarified that self reporting credit is not appropriate when a Registered Entity notifies a Regional Entity of a potential violation through a report required more quickly by another standard, such as EOP-004-1, R3. Subsequent cooperation by the Registered Entity may be considered as a separate mitigating factor in the penalty determination.
- **Human Error.** FERC will not consider “human error” as a mitigating factor in determining a penalty. FERC believes that such consideration would remove an important incentive for compliance with the NERC Reliability Standards. FERC referenced an MRO settlement where the Registered Entity made a transposition error which resulted in a violation. While the violation was a result of human error, MRO did not consider such an error as an aggravating or mitigating factor in its determination.

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

[Florida Reliability Coordinating Council](#)

[SERC Reliability Corporation](#)

[Texas Regional Entity \(Texas RE\)](#)

[ReliabilityFirst](#)

[Western Electricity Coordinating Council \(WECC\)](#)

[Southwest Power Pool Regional Entity \(SPP RE\)](#)

[Northeast Power Coordinating Council \(NPCC\)](#)

While MRO staff finds the Turlock Order instructive, MRO is concerned that the guidance that self reporting credit is not appropriate when a Registered Entity is required to report a disturbance or event may have a “chilling effect” on self reporting and the efforts underway with the Events Analysis process.

Therefore, MRO joined NERC and other Regional Entities in filing a Request for Clarification or Rehearing on this issue. The Request asks FERC to clarify that its statements were not intended to disallow self reporting of potential violations under any circumstance or to eliminate incentives to do so. Further, the Request asks FERC to retain the flexibility currently utilized by NERC and the Regions to adjust penalty amounts to account for desirable behavior where appropriate. Finally, the Request urges encouraging proactive self reporting at every juncture. If the Commis-

sion disagrees with the request for clarification, rehearing is requested on two points: 1. FERC erred in finding that Turlock did not self report the FAC-003 violation because another Standard required the load shedding associated with the event to be reported; and 2. FERC erred in concluding that self-report credit is not appropriate when there is a separate reporting obligation under a particular Standard.

MRO encourages Registered Entities to continue to self report any time they recognize possible noncompliance, regardless of whether there are required reports that must also be submitted.

A copy of FERC’s full order can be found at www.ferc.gov under Docket No. NP10-18-000.

Reliable Integration of Variable Renewable Generation Lessons Learned from the Berkeley Lab Report

John Seidel, Sr. Mgr. Situation Awareness, Event Analysis and Reliability Improvement

In December 2010, a report titled: “[Use of Frequency Response Metrics to Assess the Planning and Operating Requirements for Reliable Integration of Variable Renewable Generation](#)” was published by the Ernest Orlando Lawrence Berkeley National Laboratory (Berkeley Lab Report or Report).



This Report presents a systematic approach to identifying metrics that are useful for operating and planning a reliable system with increased amounts of variable renewable generation. It builds on existing industry practices for frequency control after an unexpected loss of a large amount of generation. The report introduces a set of metrics/tools for measuring the adequacy of frequency response within an interconnection.

The report concludes:

1. The “*declining quality of frequency control in the US is a significant reliability concern.*”
2. Addressing variable generation’s impact on frequency response, the report states there will be four impacts on the effectiveness of primary frequency control actions:
 - Lower system inertia -- although the report states

that this is a relatively minor impact at present levels of wind penetration;

- Displacement of conventional generation that is normally providing primary frequency response reserves (governor response);
 - Possible over-burdening of remaining sources of primary frequency response reserves, which can potentially become undeliverable. There is a need to closely monitor actual primary reserves;
 - The need for secondary frequency response reserves (AGC, load following) to track faster and larger ramps, and inverse ramps (load is ramping up while wind generation is declining). If secondary frequency response reserves are depleted, primary frequency control reserves that are set-aside to respond to the sudden loss of generation would necessarily be used to make up for the shortfall. The remaining primary frequency control reserves may then be inadequate to prevent operation of under-frequency load shedding following a large sudden loss of generation.
3. The report recommends that each Interconnection schedule its primary frequency response reserves (to handle a sudden loss of generation) and its secondary frequency response reserves (to handle large rapid inverse ramps of load and variable generation, etc).
 4. In the longer term, the report recommends that fre-

(Continued on page 4)

(Continued from page 3)

quency control capabilities of the interconnections should be expanded by pursuing new opportunities offered by wind generation, demand response, and energy storage.

5. The report concludes that wind generation capacity projected through 2012 in the Western and Texas interconnections can be reliably integrated, using the tools established in the report. However, the report also states [#14 on page xvii]:

“We were not able to conduct simulation studies of increased levels of variable renewable generation in the Eastern Interconnection. We found that, using the system model that was provided, we could not reproduce the frequency response of the Eastern Interconnection to a recent recorded event involving the sudden loss of a large amount of generation. The simulation results predict that the frequency response of the interconnection is much more robust than the frequency response that has been observed based on measurements of real events.”

Dynamic modeling improvements are necessary for the Eastern Interconnection (EI). More accurate/detailed data

for both load and generation is needed. To address this, NERC has created the Model Validation Task Force that reports to the NERC Transmission Issues Subcommittee. This Task Force is seeking NERC Planning Committee approval to pursue improvements in modeling data and collection techniques.

Additionally, an implementation team of the North American Synchro-Phasor Initiative is studying load modeling issues and providing their findings to the NERC Planning Committee. This group is finding that more accurate load modeling (both existing load and future load) is necessary due to its influential role in power system stability.

These modeling enhancements will take time, but efforts are underway to help identify the shortcomings of existing EI models in terms of dynamic response and frequency response. At the MRO Reliability workshop on June 21, 2011, MRO plans to include a presentation from ERCOT that describes their improvements made to the modeling process and contrast it with the EI modeling process.

The Berkeley Lab report can be found at: <http://www.ferc.gov/industries/electric-act/reliability/frequencyresponsemetrics-report.pdf>

Reliability Standard CIP-007 (v1-v4) Compliance Information

Reliability Standard CIP-007 (v1-v4), R2 states that “[t]he Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.

R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.

R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic

Security Perimeter(s).

R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

Responsible Entity’s should note that ports and services must be either enabled or disabled on a device level, and not a network level. While network level port and service management is encouraged, device level port and service management is required for compliance with the Standard.

MRO Case Notes First Quarter Update

Concurrent with the release of this Newsletter, MRO Enforcement staff posted an update to the “Case Notes” document released in January 2011. The “Case Notes” document and “2011 First Quarter Update” may be found at the following link:

<http://www.midwestreliability.org/compliance.html>.

This update includes violation descriptions and mitigation efforts for those Mitigation Plans accepted by MRO in the first quarter of 2011. Once again, the MRO Compliance Committee assisted in the development of this document

(Continued on page 5)

and provided valuable feedback. MRO staff updates the document on a quarterly basis, so please check back regularly.

For questions regarding the “Case Notes”, please contact [Sara Patrick](#), *Director of Regulatory Affairs and Enforcement*

NERC Defines “Annual” Compliance Application Notice 0010

After months of regional and industry review and comments, NERC posted the definition of “annual” in [Compliance Application Notice 0010](#) (CAN-0010) on April 19, 2011. This definition can be used for those Reliability Standards that do not include a definition of “annual.” If a Reliability Standard includes a definition of “annual,” then that definition must be followed.

For those Reliability Standards where the definition of the term “annual” is not included, each registered entity must define and document the definition of “annual.” A single definition may be used for all of the Reliability Standards requiring a definition or a registered entity may choose different definitions for each such Reliability Standards, and therefore have multiple definitions. Regardless of whether a single definition of “annual” is used or multiple definitions of “annual” are used, each registered entity must document the definition of “annual” for each Reliability Standard. According to CAN-0010, the documentation “must demonstrate that the required activity was conducted at least once in every calendar year.”

In addition, NERC provided two definitions of “annual” which can be used. Annual can be defined as follows: (1)

within a calendar year, with the calendar year beginning on January 1 and ending on December 31 (Calendar year) or (2) within a rolling twelve month period (Rolling 12 Month) therefore requiring that the activity be done once every twelve month period.

NERC notes that while the Calendar year definition could be met by performing a compliance activity in January Year 1 and in December Year 2 with twenty three months in between the compliance activities, best practices dictate registered entities conduct “annual” activities within 15 months of the previous activity. MRO agrees, but recognizes that in some cases a gap of more than 15 months may be justified. For example, for training, the time frame between compliance activities may be extended if higher quality training can be implemented rather than completing it within 15 months of the prior training.

In setting the definitions for annual it is important to keep in mind the reliability objective, which is to “ensure that entities perform a particular task on a regular basis, with an established maximum interval between the occasions when the task is performed.”

Recent Cyber Attacks Should Elevate Awareness Cybersecurity a Top Priority

DOE laboratory says it was victim of an Advanced Persistent Threat designed to steal technical data

An article in [Computerworld](#) on April 19th, 2011, reported that the Oak Ridge National Lab (a Department of Energy-funded Lab) was forced to shut down its email systems and internet access following a “sophisticated cyberattack.” The Oak Ridge National Laboratory is home to one of the world’s most powerful supercomputers. The article reports that “several other national laboratories and government organizations were targeted in the same attacks, which appear to have been launched earlier this month,” and that “initial investigations showed that those behind the attacks were attempting to steal technical data from the lab’s system and send it to an external system.”

The attack was apparently carried out through a phishing email sent to lab employees disguised as a request from the company’s HR Department. Employees were asked to click

on a link for more information related to benefit changes, resulting in a malware program being downloaded on their systems. This attack, along with the recent [RSA breach](#) that happened earlier in April, provide evidence that cyber attacks on our information and technology systems are real and imminent threats. And as such, securing our cyber systems must be a top industry priority.

Every email and internet user within your organization plays a role in ensuring data and information security. Communication, along with employee training and education, are key components in raising employee awareness and preventing cyber attacks.

For more information on promoting cybersecurity awareness in your organization, visit the [Department of Homeland Security](#) website.

The Checklist Manifesto ■ How To Get Things Right

A book by Dr. Atul Gawande

By Miggie Cramblit, General Counsel and Director of External Affairs

Dr. Atul Gawande is an accomplished writer¹, doctor and policy advisor.² The thesis of his latest book “The Checklist Manifesto · How to Get Things Right (“Checklist”)³, is that checklists improve outcomes in extremely complicated matters.

In his pursuit of improving surgical outcomes worldwide through his work with the World Health Organization, he concluded implementing a checklist for the operating room was the solution. His work showed post checklist, major surgical complications fell by 36% and deaths by 47% across hospitals with abundant to very modest resources.⁴ With examples from various industries airline, construction, medicine, private equity, restaurants and Wal-Mart, he persuasively makes his point.

Construction of a skyscraper requires thousands of tasks and a multitude of trades with hundreds of people on site daily to complete the building. Interviewing a project executive, Gawande learned two checklists were used a task check list and a communication checklist. Gawande observes:

[W]e trust in the ability of the experts to manage the complexities. They in turn know better than to rely

on their individual abilities to get everything right. They trust instead in one set of checklists to make sure that simple steps are not missed or skipped and in another set to make sure that everyone talks through and resolves all the hard and unexpected problems.⁵

The importance of the checklist lies not only in making sure routine, repetitive and critical details are not overlooked, but the process of using it and communicating fosters teamwork and early identification of potential problems. Dr. Gawande relates a story of removing an adrenal gland – he had removed about forty without complication. The checklist required him to discuss blood loss with the surgical team. He said he didn’t expect much, but noted because of the location of the tumor there was at least a theoretical concern. The nurse noted it and reserved blood, which the patient, who almost died, needed.⁶ The checklist forced discipline to think and communicate about the procedure and the group to start to come together as a team. Each member of the team was a technical expert, but their job was not just performing individual tasks “but also helping the group get the best possible results.”⁷

(Continued on page 7)



NERC Case Notes

NERC now has 45 [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 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 posts Lessons Learned from Event Analysis

NERC makes lessons learned from Event Analysis available to industry on their [website](#).

NERC Compliance Application Notices

Also on NERC’s website, you will find [Compliance Application Notices](#) or CANs. NERC CANs have two purposes. The first purpose is to assist Compliance Operations and Regional Entities with the performance of compliance activities. The second purpose is to assist registered entities with compliance regarding NERC Reliability Standards.

(Continued from page 6)

Gawande, also discusses Wal-Mart's response to Katrina which was lauded by Harvard's Kennedy School of Government. Gawande notes "[i]n response to risk, most authorities tend to centralize power and decision making,"⁸ he advocates pushing "the power of decision making out to the periphery and away from the center. You give people the room to adapt, based on their experience and expertise. All you ask is that they talk to one another and take responsibility." New Orleans Wal-Mart employees were instructed: "Make the best decision that you can with the information that's available to you at the time, and, above all, do the right thing."⁹ Executive management acknowledged that "[a] lot of you are going to have to make decisions above

your level."¹⁰ Rather than issuing orders in a complex constantly changing environment, executive management set goals, measured progress and most important made sure people talked to each other. Checklists function the same way.

To Gawande's list of accolades for checklists, I would add two. The process of developing the checklist creates discipline and focus and having the checklist creates the opportunity to continuously improve and adapt it.

Whether preparing for your organization's board meeting, a compliance audit or a regulatory filing, this book offers evidence-based practical solutions to improve your results. It's an enjoyable and quick read.

¹ He has been a staff writer for the New Yorker, winning the 2010 National Magazine Award for Public Interest writing for his New Yorker article, "The Cost Conundrum." His New Yorker article "Letting Go" is a 2011 National Magazine Awards finalist. "Complications: A Surgeon's Notes On An Imperfect Science" was a 2002 National Book Award finalist and has been published in over one hundred countries. In 2006, he received the MacArthur Award for his research and writing. "Better: A Surgeon's Notes On Performance" was one of Amazon.com's ten best books of 2007. The subject of this review is his newest book, "The Checklist Manifesto · How to Get Things Right," which is currently number 17 on the New York Times non-fiction hardcover bestseller list.

² He's a staff member at Brigham and Women's Hospital and the Dana Farber Cancer Institute. He served as a senior health policy advisor in the Clinton presidential campaign and White House from 1992 to 1993, and the New Yorker magazine. He received his B.A.S. from Stanford University, M.A. (in politics, philosophy, and economics) from Oxford University, M.D. from Harvard Medical School, and M.P.H. from the Harvard School of Public Health.

³ Atul Gawande, *The Checklist Manifesto · How to Get Things Right* (New York: Metropolitan Books Henry Holt and Company, 2009)(Checklist), 72.

⁴ *Id.*, 154. / ⁵ *Id.*, 70. / ⁶ *Id.*, 191. / ⁷ *Id.*, 103. / ⁸ *Id.*, 73. / ⁹ *Id.*, 76. / ¹⁰ *Id.*

EXTERNAL AFFAIRS UPDATE

Miggie Cramblit, General Counsel and Director External Affairs

During the next several months, I will be visiting the state public utility/service commissions to formally introduce MRO and the NERC structure, and the demands it places on the Registered Entities that those commissions regulate. Another purpose for the visits will be to open a channel of communication between MRO and the commissions given there is a shared interest in reliability.

I've developed a presentation with feedback from the board, and will also be reaching out to Registered Entities and commission staff prior to my visiting a particular state to ensure the presentation meets the commission's needs.

I can be contacted regarding this effort at me.cramblit@midwestreliability.org

OPERATIONS UPDATE

Dan Schoenecker, VP Operations

NERC ROW Clearance Alert Update

NERC recently drafted a letter to Transmission Owners (TOs) and Generation Owners (GOs) providing additional guidance on prioritizing the transmission facilities for right of way clearance assessments and identifying NERC's expectations for performing the assessments. This draft was shared with industry trade groups who provided valuable input on the details of the message and on the plan for subsequent periodic reporting on the status of the assessments. What was initially characterized as a letter, has now been drafted as a document titled "NERC Facility Design, Connections, and Maintenance (FAC) Assessment Plan Review Criteria." The updated document was sent to the trade groups on April 26th, 2011 for final review and comment. After final edits are made, the document will be posted on the NERC Alerts webpage on May 11th, one day prior to a webinar scheduled on May 12th from 12-2

pm central time to review the criteria document.

Beginning the week of May 2nd, MRO will begin sending letters to the TOs and GOs who have provided acceptable assessment plans. Following the webinar, MRO will contact the remaining TOs and GOs to provide feedback on the assessment plans they've submitted. Regional Entities will also provide a spreadsheet template to the TOs and GOs to document the results of the transmission circuits that have been assessed, along with any plans for mitigating issues that were discovered. The first update on the status of the assessments will be due from the TO's and GO's in mid-July.

Event Analysis Process

NERC held a webinar on April 14th to discuss version 2 of the Event Analysis Process document prepared by the NERC Event Analysis Working Group (EAWG). Version

(Continued on page 9)

MRO Board Spotlight

Vice-Chair, Jeffrey J. Gust

Jeffery J. Gust PE

VP Compliance and Standards

MidAmerican Energy Company

Jeff's role as VP Compliance and Standards at MidAmerican Energy Company is to manage the company's FERC mandatory reliability standard compliance requirements, state mandatory electric distribution and gas pipeline standard requirements and develop and manage the company's transmission planning and services strategy and requirements through the Midwest ISO processes. His staff includes managers and directors working on FERC reliability standards, state gas pipeline and electric distribution standards, transmission system planning, and transmission services. Jeff enjoys the technical challenges associated with the ongoing changes to the reliability standards as well as the infrastructure policy work that is facing North America today.

Jeff graduated from Iowa State University in 1985 with a Bachelor of Science Degree in Engineering Science and obtained his Iowa mechanical engineering professional engineering license in 1990. After graduating from Iowa State University, Jeff went to work for Iowa Electric Light and Power Company for four years in the engineering department as a mechanical engineer. In 1990, he joined Iowa Power Inc., a predecessor company to MidAmerican, as a Production Analysis Engineer. In April 1999, Jeff was promoted to Vice President - Electric Trading. In August 2004, he was promoted to Vice President - Energy Supply Management. During the next five years, Jeff was responsible for managing MidAmerican's electric trading, gas supply, gas operations, and fuel and transportation functions. In August 2009, Jeff moved over to the compliance and planning department and was named VP Compliance and Standards.

Jeff and his wonderful wife Linda have been married for 21 years. They have one daughter in high school in West Des Moines, Iowa. Jeff enjoys woodworking, running, skiing, boating and many other outdoor activities.

MRO GOVERNANCE - THE BOARD OF DIRECTORS

Jessica Mitchell, Assistant Corporate Secretary

The MRO Board of Directors last met on March 24, 2011, in Bloomington, MN. The agenda, highlights, and draft minutes from that meeting can be found on MRO's [web-site](#).

Although the full list of board actions can be found in the meeting minutes, there are two of significance worth highlighting here. First, at the recommendation of the MRO Planning Committee, the board retired the Reliability Assessment Subcommittee (RAS). The RAS was initially created to perform probabilistic adequacy studies for the MRO region to support the proposed MRO adequacy standard, which has since been withdrawn. The adequacy analysis is now being performed by other industry groups such as the Midwest ISO (MISO).

Second, at the recommendation of staff and the MRO Security Committee, the board retired the Security Committee as a result of overlaps in responsibility between the MRO Standards and Security Committees (more information on page 10 of this newsletter). Matters pertaining to education, sharing of best practices, and providing guidance on security-related matters to entities in the MRO Region will

be provided under other MRO organizational groups. The board encouraged existing Security Committee members to utilize their expertise and seek membership on other committees and working groups.

Also at the meeting, the board continued its spotlight on *Reliability Excellence*. Mr. Mark Gutzmann, Manager, System Protection Engineering at Xcel Energy, provided meeting attendees with an overview and lessons learned involving Xcel Energy's recent peer review, benchmarking, and process improvements of its system protection program across Xcel Energy's operating companies. Mr. Gutzmann's presentation was well received by meeting attendees and is provided on MRO's [website](#).

The next board meeting is scheduled for **Thursday, June 16, 2011**, at the Hilton Airport Hotel in **Bloomington, MN**. Tim Gallagher, president of *ReliabilityFirst*, and NERC Trustees; Tom Berry and Paul Barber, will be in attendance.

Meetings are open to the public and staff and the board encourage your attendance. A current board roster, along with meeting details, can be found on MRO'S [website](#).

OPERATIONS UPDATE, cont...

(Continued from page 7)

2 is posted on NERC's website at: <http://www.nerc.com/page.php?cid=5365>.

A question and answer session was included in the webinar and will also be posted at the above website. Version 2 will be implemented with Phase 2 of the field test of the event analysis process, which begins on May 2, 2011. Some of the changes in the process include a "24 hour no-

tification" requirement, an update of the event categories, updates of timelines for various process steps, and additional clarification on the process steps and NERC's expectations.

Please contact MRO staff (Dan Schoenecker, John Seidel, Bill Kunkel) with any questions. Events in the MRO Region should be reported to the following address: events@midwestreliability.org

STANDARDS UPDATE

Carol Gerou, Standards Manager



Expedited Revisions to CIP-005-3

The expedited revisions to CIP-005-3 ("Cyber Security–Electronic Security Perimeter (s)") have resulted in a [CIP-005-4 draft 2](#) which is out for comment and ballot period until April 28, 2011. Most of the revisions center around requirement 6, "Interactive Remote Access Controls."

This requirement indicates

that a responsible entity that allows access to Cyber Asset (s) within its electronic security perimeter(s) shall establish, document, implement and maintain **Interactive remote access** controls.

Interactive remote access is user interactive access by a person, used for **support or maintenance**, which originates from a Cyber Asset which is not **an intermediate device**, and not located within any of the Responsible Entity's Electronic Security Perimeter(s), whether network-based or dial-up access. Remote access can be initiated from: 1) Cyber Assets used by the Responsible Entity; 2) Cyber Assets used by employees; and 3) Cyber Assets used by vendors, contractors, or consultants.

Support or maintenance includes non-operational activities associated with the upkeep, testing and modification of Cyber Assets or networks within the Electronic Security Perimeter. Examples of support or maintenance activities include, but are not limited to, configuration changes, power system model maintenance, vulnerability assessments, incident response, troubleshooting, computer system monitoring, and application of software patches.

An **Intermediate device** is a Cyber Asset that is 1) used to provide the required multi-factor authentication for the interactive remote access; 2) is a termination point for the required encrypted communication; and 3) restricts the interactive remote access to only authorized users. Intermediate devices are sometimes called proxy systems. The

functions of an intermediate device may be implemented on one or more Cyber Assets. The intermediate device may be located outside the Electronic Security Perimeter, as part of the access control device (firewall) on the Electronic Security Perimeter, or in a DMZ network.

This documented **Interactive remote access control** shall include: 1) An intermediate device such that the Cyber Assets initiating interactive remote access do not have direct access to Cyber Asset(s) within the Electronic Security Perimeter (**R6.1**); 2) Interactive remote access such that communications between the Cyber Asset initiating interactive remote access and the intermediate device(s) are encrypted (encryption for dial-up connections is required only where technically feasible) while using a network that is shared with users not associated with the Responsible Entity (**R6.2**); 3) Interactive remote access such that multi-factor authentication is required for all interactive remote access between the originating Cyber Asset and the intermediate device, where technically feasible (**R6.3**); and, 4) An **Interactive remote access user policy** (**R6.4**).

An **Interactive remote access policy** shall include: 1) Specific language in the interactive login banner on the intermediate device for remote access which requires acknowledgement and adherence to the controls specified interactive remote access user policy, where technically feasible (**R6.4.1**); 2) Update anti-malware software on Cyber Assets used to initiate the interactive remote access, consistent with CIP-007-4 Requirement R4, before a successful connection is completed (**R6.4.2**); 3) Update patch levels for operating system and applications used to initiate the interactive remote access, consistent with CIP-007-4 Requirement R3, before a successful connection is completed (**R6.4.3**); 4) Prohibit VPN "split-tunneling" or "dual-homed" workstations (which can concurrently access multiple networks) when performing interactive remote access (**R6.4.4**); and 5) For vendors, contractors, or consultants: include language in contracts that binds all interactive remote access Cyber Assets to comply with items 6.4.2, 6.4.3 and 6.4.4 of this list (**R6.4.5**).

Comments were due to NERC by April 28, 2011 at the following link: <http://www.nerc.com/filez/standards/SAR-Urgent Action Revisions%20to%20CIP-005-3.html>

STANDARDS UPDATE, *continued...*

MRO Security Committee Retired

In September 2010, the MRO Security Committee sought guidance from the board on how its role and future activities could continue to provide value to the region. The board directed the committee to review its charter, along with the charters of other industry security committees, and provide the board with a recommendation as to how this committee may be best utilized in the future.

To support the Security Committee in this effort, MRO staff provided an assessment that compared the Security and Standards Committees' roles and responsibilities. The comparison found a significant amount of overlap between both committees' charters relating to their work with Reliability Standards, training and education, and guidance to stakeholders on CIP standards. Because of this overlap, the Security Committee recommended to the board at the March 24, 2011 board meeting, that it retire and integrate the expertise of its members with the Standards Committee, NERC Standards Review Subcommittee (NSRS), and the MRO CIP Subject Matter Expert (CIP SME) group. The board approved the recommendation, and a discussion on the integration will occur at the Standards Committee meeting on May 19th, 2011.

Additional details on the committee's recommendation to the board can be found in the board meeting agenda packet on MRO's website at: http://www.midwestreliability.org/ABO_bod_agenda_minutes.html.

One of the key roles of the Security Committee was to provide input to the three MRO representatives on the NERC Critical Infrastructure Protection Committee (NERC CIPC), to ensure the region's voting position is

represented on white papers, guidance documents, and other NERC CIPC projects. This key role will continue by utilizing the expertise of the Standards Committee, NSRS, and CIP SME working groups.

One of the Standards Committee's key initiatives is to provide non-binding assistance to stakeholders in understanding the application of NERC Reliability Standards through communication, education, and training. A strategy for driving the initiative is establishing Subject Matter Expert (SME) groups that share their knowledge and expertise to develop application guides, and training tools for stakeholders. In addition, the Standards Committee and its subcommittee will utilize SME groups for additional assistance and comments on existing, new, or emerging Reliability Standards. Integrating the expertise of Security Committee members with these various groups will help strengthen and drive the Standards Committee's key initiative and goal to becoming a respected resource for stakeholders in the industry.

A CIP SME Volunteer Needed!

The MRO Standards Committee is looking for SMEs in the Critical Infrastructure Protection area (which covers the NERC Reliability Standards CIP-002 through CIP-009). SME's are required to...

If you are such an expert, or know someone who is, and would like to volunteer for this opportunity please fill out a [nomination form](#) and send it to Jennifer Matz. (j.l.matz@midwestreliability.org)

FINANCE UPDATE

*Sue Clarke,
VP of Administration and Finance*

2010 Audited Financials



MRO's independent auditor, Baker Tilly, completed their audit of MRO's 2010 financials and reported the audit as smooth, and provided MRO a "clean" opinion. The MRO Board of

Directors accepted the 2010 audited financials at the March 24, 2011 board meeting, which can be found on the MRO website at http://www.midwestreliability.org/ABO_overview.html.

NERC and the Regions 2012 Business Plan and Budget

This year, NERC and the Regions revised the Business Plan and Budget Three Year Common Assumptions to reflect four years. The common assumptions were devel-

oped as an effort to ensure consistency amongst NERC and the Regions' business plans and budgets.

On May 9th, NERC will post Draft 1.0 of the 2012 Business Plan and Budgets submitted by all eight Regional Entities. The same day, MRO will post its 2012 Business Plan and Budget on MRO's website for stakeholder review and comment. On June 16th, MRO will seek final approval of MRO's 2012 Business Plan and Budget from the board. The Regional Entities final budgets are due to NERC on July 8th. The NERC BOT will review the Regional Entities final budget submittals for approval on August 4th, and then submit NERC and the Regions final budgets to FERC for approval on August 24th.

*Any questions on the above 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.

ENFORCEMENT UPDATE

Jacob R. Phillips, Enforcement Attorney

Tracking Enforcement Actions

Generally, there are eight steps in the MRO enforcement process. In an effort to assist Registered Entities' understanding of the steps in the process, this article provides an overview of each step.

Step 1: Initial Review & Reliability Assessment

MRO Compliance staff may identify a possible violation (PV) through one of the eight discovery methods outlined in Section 3 of the Compliance Monitoring and Enforcement Program (CMEP). The discovery methods include: compliance audits, self-certifications, spot checks, compliance investigations, self-reports, periodic data submittals, exception reports, and complaints. Once MRO Compliance staff identifies a PV, then MRO Enforcement staff conducts an independent review of the findings.

Step 2: Issue NOPV or Dismiss

Upon completing the independent review, MRO Enforcement staff either validates or dismisses the PV. If the PV is validated, MRO Enforcement staff issues a Notice of Possible Violation (NOPV). The NOPV includes a brief description of the PV, and instructs the Registered Entity to retain and preserve all data and records relating to the PV. If the PV is dismissed, MRO Enforcement staff issues a Notice of Dismissal to the Registered Entity and the enforcement action is closed.

Step 3: Review Facts & Circumstances

If MRO determines that a PV may have occurred, and an NOPV is issued, then MRO Enforcement staff continues to work closely with the Registered Entity to determine the full scope of the violation. Concurrently and apart from Enforcement staff, MRO Mitigation staff works closely with the Registered Entity in order to determine the best method for mitigating the actual and potential risks posed by the PV.

Step 4: Issue NAVAPS or NAC

Upon completing a full review of the facts and circumstances, MRO Enforcement staff either prepares a Notice of Administrative Citation (NAC) or a Notice of Alleged Violation and Proposed Penalty or Sanction

(NAVAPS). MRO may issue a NAC¹ if it determines that the violation poses a minimal risk to the Bulk Power System (BPS), otherwise MRO may issue a NAVAPS. In either case, the Registered Entity has 30 days to respond to the Notice or MRO will deem the Registered Entity to have accepted the determination of violation and proposed penalty or sanction.

Step 5: Issue NOCV or Settlement

Upon acceptance by a Registered Entity of an Alleged Violation or the expiration of time for responding to the NAVAPS, a violation becomes a Confirmed Violation. If a NAVAPS was issued, then the MRO Enforcement staff issues a Notice of Confirmed Violation (NOCV). If a NAC was issued, then it is submitted to NERC for review.

At any point in the process, a Registered Entity may request to enter into settlement discussions. The request may be made verbally or in writing (letter or email). Upon receipt of a request for settlement, MRO Enforcement staff prepares an Acknowledgement of Request for Settlement. Upon reaching an agreement with a Registered Entity, MRO Enforcement staff presents the Settlement Agreement to the MRO Hearing Body for approval.

Step 6: NERC Staff Review

Once a NOCV, NAC, or Settlement Agreement is finalized, MRO Enforcement staff reports the enforcement action to NERC. Upon review, NERC staff drafts and finalizes a Notice of Penalty (NOP) and provides any comments back to MRO Enforcement staff.

Step 7: BOTCC Review

After the enforcement action review is complete, NERC staff presents the enforcement action and a draft NOP to the NERC Board of Trustees Compliance Committee (BOTCC).

Step 8: NOP Filing at FERC or Canadian Authority

Upon approval of the BOTCC, the NOP is filed with the Federal Energy Regulatory Commission (FERC) and becomes publicly available. These NOPs are posted on the NERC website² with links to the accompanying Or-

(Continued on page 12)

¹ Please refer to the MRO MATTERS March/April 2011 Newsletter for further information on the various factors considered in determining whether a violation qualifies for a Notice of Administrative Citation, available at: http://www.midwestreliability.org/06_news/newsletters/2011/Newsletter_Mar_2011.pdf.

ENFORCEMENT UPDATE, cont...

ders approving the actions. Additionally, Registered Entities may track the filings and Orders by subscribing to the FERC docket.³ The FERC docket numbers are available on NERC's website.⁴

Please note, this process is different in the Canadian provinces. In Saskatchewan, the Saskatchewan Oversight Authority has the legislative authority to enforce compliance with adopted reliability standards. In Manitoba, the Public Utilities Board approves any enforcement actions proposed by MRO.

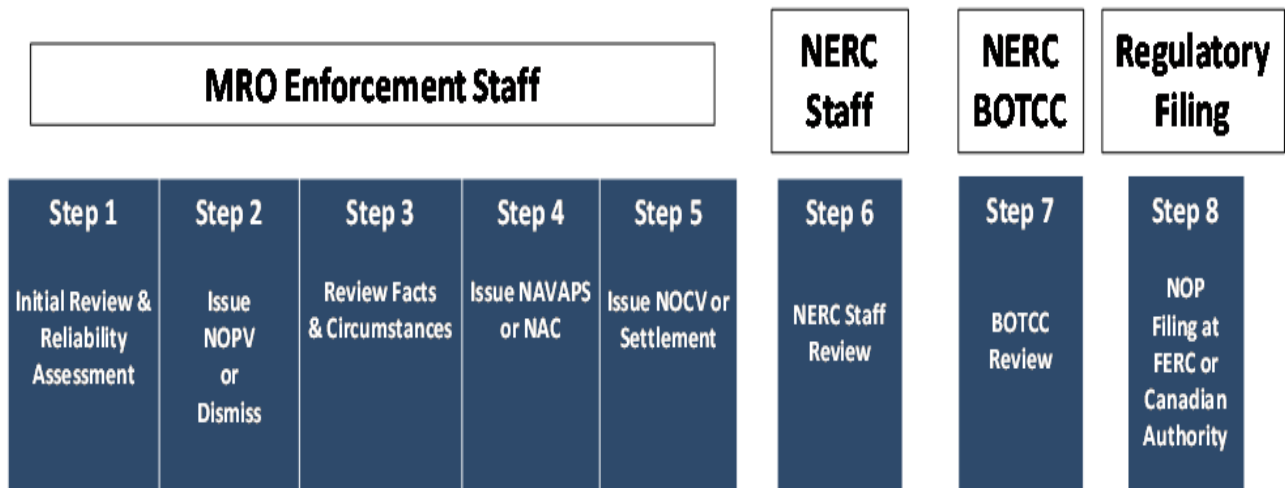
Throughout the enforcement and mitigation process, MRO

works closely with the Registered Entity, NERC, and other Regional Entities to improve reliability and solve problems. MRO continuously strives to develop more effective and efficient enforcement processes -- your suggestions are always welcome.

Any questions, comments or suggestions may be directed to the MRO Enforcement Department.

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

Violation Processing Steps



See <http://www.nerc.com/filez/enforcement/index.html>.

See <http://www.ferc.gov/docs-filing/esubscription.asp>.

See <http://www.nerc.com/filez/enforcement/index.html>.

Quote of the Month

“If you don't learn from your mistakes, there's no sense making them”

-Anonymous

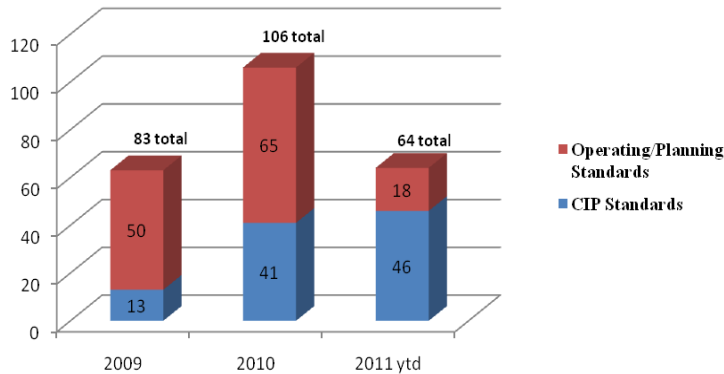
CMEP Report

MRO Compliance Monitoring and Enforcement

May 2011

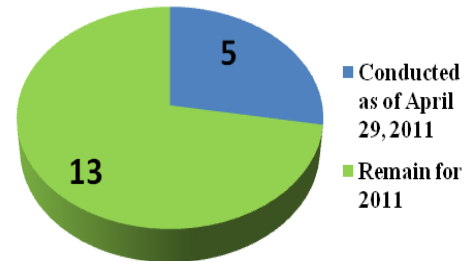
Reliability Standards Violation History

(Number of Possible Violations reported to NERC)



Compliance Audit Status

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



Standards Most Frequently Violated

(numbers below do not include dismissals)

Standards Most Frequently Violated	Frequency	% to Total
PRC-005-1 Trans. and Gen. System Maint. and Testing	60	25%
CIP-004-1 Cyber Security-Personnel and Training	26	11%
PRC-008-0 Implementation and Documentation of UFLS Equip. Maintenance Program	22	9%
CIP-007-2 Cyber Security--Systems Security Management	22	9%
FAC-003-1 Vegetation Management	13	5%

ANNUAL IMPLEMENTATION PLAN UPDATE

Wayne VanOsdol, Vice President Compliance

The 2011 annual implementation plan and associated compliance audit schedules (and other monitoring methods) can be found on the MRO website at: [MRO 2011 Implementation Plan](#). In 2011, MRO is piloting more performance observations (ex: physical inspections) to test compliance in the field. Registered Entities have been very cooperative in assisting MRO staff to coordinate the work in the field. Also, MRO is initiating CIP spot checks as a follow-up to the work done in 2010. These CIP spot checks include three parts:

CIP-002-3 Spot Check

MRO continues to enhance the compliance program by incorporating performance monitoring processes. In June, MRO will begin conducting CIP-002-3 spot checks in preparation for entities scheduled to receive an audit in the near future. Conducting the spot check prior to the audit will allow CIP auditors the ability to obtain a thorough understanding of the assets in which the entity has placed

cyber and physical controls. In addition, the spot check has been expanded to incorporate information similar to the NERC Sufficiency Review process, and to include a questionnaire pertaining to the DOE "21 steps to improve cyber security." Information obtained during the spot check will be used for the audit to ensure duplication of work does not occur.

Annual Self-Certification Update

On April 14, 2011, MRO notified the Registered Entities who were scheduled to participate in the spring annual self-certification; those Registered Entities not contacted are scheduled to participate in the fall annual self-certification. The 2011 annual self-certification procedures (spring and fall) can be found on the MRO website at: [MRO 2011 Annual Self Certification Procedure](#).

CIP- Technical Feasibility Exception (TFE)

MRO continues to manage the TFE processing as required.

(Continued from page 13)

Education and Training

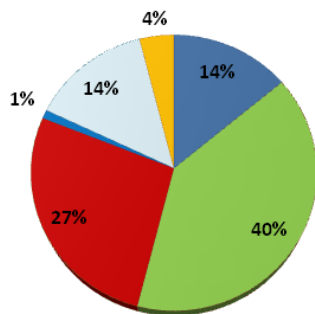
MRO will hold a Reliability Conference on June 21 and 22, 2011 at which Reliability Standard Subject Matter Experts will present information pertaining to the application of the Standards with emphasis on the CIP standards. More information and registration for this workshop can be found at the following web link: http://www.midwestreliability.org/events_June_2011.html. In addition to the Reliability Conference being held in June, MRO will hold a CMEP workshop on December 14, 2011; more information to follow regarding this workshop.

WebCDMS Update

MRO utilizes the Dashboard feature in webCDMS to notify Registered Entities of information related to webCDMS as well as other compliance related information. Please check the dashboard frequently. MRO will continue to send e-mail notices to the Primary Compliance Contacts when information is posted on the Dashboard.

Comparison by Discovery Method (June 18, 2007 through April 29, 2011)

■ Self-Certification
■ Audit
■ Spot-Check
■ Self-Report
■ Data Submittal
■ Compliance Investigation



Discovery Method Detail	June 18 - Dec 2007	2008	2009	2010	2011 YTD	Sub Total	(-less) Dis-missed	Total
Self-Certification	33	2	11	2	0	48	14	34
Self-Report	9	19	12	48	25	113	17	96
Compliance Audit	3	9	36	35	0	83	19	64
Compliance Investigation	0	0	0	0	10	10	0	10
Data Submittal	1	0	0	0	0	1	0	1
Spot-Check	0	0	7	46	0	53	18	35
Totals	46	30	66	131	35	308	68	240

Status of Alleged and Confirmed Violations Process

	Total ⁽¹⁾	%
Total Number of Alleged Violations	308	100%
Less: Number of Dismissals	68	22%
Less: Number of Violations Awaiting NOP	4	1%
Less: Number of Violations Processed ⁽²⁾	122	40%
Number of Violations Outstanding ⁽³⁾	114	37%
Total Completed	190	62%

1. Numbers are a cumulative total
2. Accepted or approved by applicable regulator, includes NOCV's, settlements, and administrative citations.
3. Includes both alleged and confirmed violations yet to be processed and approved by applicable regulator (308less68 (Dismissed) less122 (accepted and/or approved by regulator) less 4 (viols awaiting NOP)=114)

MRO staff continues its validation of alleged violations that are identified through the eight discovery methods (compliance audit, self-certification, random spot-check, compliance investigation, self-report, data submittal, exception reporting, and complaints) according to the rules. Any alleged violation determined to be valid by MRO staff is tracked through completion of the mitigation as outlined in an accepted mitigation plan.

All mitigation plans have been submitted as required per the CMEP guidelines. If an entity does not believe it will meet the proposed completion date provided in the accepted mitigation plan, an extension of time may be requested. The extension process is described in the CMEP. Registered Entities that do not meet the proposed completion date or other milestones outlined in their plan may be subject to additional penalties and/or sanctions. It is very important to meet the milestones in the mitigation plan.

Status of Mitigation Plans

Mitigation Plans	
Number of Violations with Mitigation Plans	156
Number of Violations with Completed Mitigation Plans (validated by MRO staff)	136
Number of Violations with Outstanding Mitigation Plans to be Completed by the Registered Entity	20
Number of Late Mitigation Plans	0
Number of Violations with Mitigation Plans to be Submitted and Accepted by MRO	84

OTHER COMPLIANCE UPDATES

Wayne VanOsdol, Vice President Compliance

Revisions to Audit Reports – Making Reports More Meaningful

Based on feedback received from Registered Entities, trades associations, and MRO staff, the compliance audit report was modified to be more readable and more meaningful to the reader. The structure, format, and content is substantially different when compared to past audit reports.

Key changes include:

- The organization section was changed to flow in a more logical manner.
- The report highlights the applicable standards under the compliance audit scope, rather than in a table format where finding determinations (yes or no) were listed. In addition, the title of each standard is listed, rather than just identifying the standard ID number.
- The report highlights the findings discovered, with a detailed description explaining why the finding is a possible violation.
- The report includes recommendations to help improve compliance and notable observations to reinforce good practices.
- The report includes hyperlinks for background information.

Performance-Based Principles in Conducting Our Work

MRO is moving towards performance-based principles in its compliance work – we call it “operationalizing compliance.” While documentation is important to a compliance program, performance is paramount, and is a means of moving compliance from the “office” and “paperwork,” to the field.

Operational compliance pertains to monitoring the imple-

mentation (or obtaining evidence of implementation) of internal controls associated with the applicable Reliability Standard(s). (i.e., performance monitoring.) Performance monitoring can take place by conducting field inspections or observing performance such as the conduct of training.

Not all performance requires MRO staff to be in field. For example, we plan to conduct a “maintenance and testing compliance spot-check” on the device that was the root cause of a misoperation. MRO staff believes we can strengthen reliability through the compliance program by adding key elements of performance by way of observations, physical inspection, and validation of internal controls being implemented by the Registered Entity.

This does not necessarily mean more work for Registered Entities; it does however, mean more work for MRO staff as we will need to carefully plan our work on those items which may be most important to reliability. Moving towards more risk-based approaches through performance-based principles will readjust focus on matters of significance to reliability.

In April 2011, MRO initiated an “ATC/AFC Flow Gate Path Annual Data Submittal” for the new Reliability Standards MOD-001, MOD-004, MOD-008, MOD-028, MOD-029, and MOD-030. The compliance team will conduct a performance validation using data that can be accessed via OASIS. This represents an example of performance monitoring and the ability to monitor new standards without expanding the scope of the audit.

We will continue to keep Registered Entities informed on the progress of this key program enhancement. There is much more to the effort, so please stay tuned.

The MRO Compliance Department can be reached at mco@midwestreliability.org

IMPORTANT INDUSTRY UPDATES AND EVENTS

NERC Testifies at Energy and Power Subcommittee Hearing

WASHINGTON, DC – on April 7, 2011, Gerry Cauley, President and Chief Executive Officer of the North American Electric Reliability Corporation (NERC), testified to the Subcommittee of Energy and Power on NERC's 2010 assessment, Resource Adequacy Impacts of Potential U.S. Environmental Regulations. Read the full [press release](#).

NERC CEO Speaks on Electric Infrastructure Security Summit Panel

WASHINGTON, DC - NERC President and CEO, Gerry Cauley, participated in a panel discussion at the Electric Infrastructure Security Summit on April 11-12 in Washington, DC. The conference brought together government and industry leaders to enhance cooperation and coordination of electromagnetic threat efforts and discuss new information and protection options for critical infrastructures. Read Mr. Cauley's [remarks](#).

Cauley Testifies at House Homeland Security Subcommittee Hearing

WASHINGTON, DC - On April 15, NERC President and CEO, Gerry Cauley, testified in front of the House Committee on Homeland Security's Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies. Read Mr. Cauley's [testimony](#).

FERC reaffirms order requiring revised definition of bulk electric system

WASHINGTON, DC - On March 17, the Federal Energy Regulatory Commission (FERC) issued an order (RM09-18-001) reaffirming that the definition of "bulk electric system" must be revised to eliminate the unchecked regional discretion that has resulted in inconsistencies and accepting revised procedures for developing mandatory reliability standards. The full press release can be found on FERC's [website](#).

Department of Energy, Duke Energy and EPRI Partner to Test Advanced Energy Technologies for Utilities

WASHINGTON, DC - The Department of Energy (DOE) announced on April 14, that the DOE's Advanced Research Projects Agency-Energy (ARPA-E) has signed a partnership deal with Duke Energy, one of the largest electric power companies in the United States, and with the Electric Power Research Institute (EPRI), a non-profit research organization that focuses on the electric power utility industry in the U.S. and abroad, to

identify opportunities for testing and deploying ARPA-E funded projects that will bolster the electric grid. [Read more.](#)

CONFERENCE: Managing SCADA Security Risks 2011

Wednesday May 25, 2011 - Thursday May 26, 2011
San Francisco

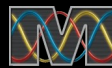
.SCADA systems are becoming prey to increasingly sophisticated security threats due partly to the actual amount of connections but also to potential new vulnerabilities within the business network itself – including those that could impact trade secrets, proprietary information and the functionality of the business itself. [Read more.](#)

Related Links:

[Department of Energy](#)

[Federal Energy Regulatory Commission](#)

[North American Electric Reliability Corporation](#)



MIDWEST RELIABILITY ORGANIZATION

Presents a Learning Event



RELIABILITY CONFERENCE

June 20-21, 2011 ■ Embassy Suites ■ Bloomington, MN

CONFERENCE OVERVIEW

The North American Bulk Electric System is the largest interconnected system in the world—owned and operated by multiple organizations across multiple state and federal seams. Meeting reliability expectations has become increasingly complex with the new issues emerging regularly related to generation, transmission and security.

This conference is designed to educate registered entities in the MRO region on topics related to protection systems, reliability metrics, cyber security applications, the new UFLS standard, planning and assessments, and other technical matters related to reliability of the bulk electric system.

KEY RELIABILITY TOPICS:

Day One

Fill-In-The-Blank Standards - Carol Gerou, MRO

Reliability Assessment and Performance Analysis - Mark Lauby, NERC

Reliability Metrics - Bill Adams, Southern Company

Mis-Op Reporting - Dan Jesberg, MRO

Under Frequency Load Shedding Transition to Planning Coordinator - TBD

Event Analysis - Dan Schoenecker, MRO

NERC Modeling Improvement Initiative - Bob Cummings, NERC

ERCOT Modeling - Woody Rickerson, ERCOT Grid Coordination

Reliability Assessments - Josh Collins, Midwest ISO & Pete Koegel, MAPPOR

Special Protection Systems Criteria - John Seidel, MRO

PRC Standards Application Guidance - MRO PRC SME Working Group

Day Two

Critical Infrastructure Protection Standards Application Guidance - MRO CIP SME Working Group

22 Steps to Improve Cyber Security of SCADA Networks - Chris Kulseth, MRO

CONFERENCE DETAILS

Who should attend this conference? A complete agenda, including additional details on the reliability topics and registration information, can be found on our website at: <http://www.midwestreliability.org/meetings.html>

There is no fee for attendance!

EVENT LOCATION

Embassy Suites Airport Hotel
7901 34th Avenue South
Bloomington, MN

A block of rooms has been reserved at \$159 per night for a two room suite. To make a reservation, you may call 1-800-EMBASSY and request the group rate of Midwest Reliability Organization

The deadline for this reduced rate is **May 31, 2011.**

NEARBY HOTELS

Crown Plaza Airport Hotel
952-854-9000 (ask for the MRO rate of \$108 - #100228113)

Hilton Bloomington Airport Hotel
952-854-9000 or www.msppairport.hilton.com



MRO 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, Regulatory Affairs, Counsel and Enforcement Director](#) (1708)
[Jacob Phillips, Enforcement Attorney](#) (1758)
[Janice Anderson, Enforcement Admin](#) (1720)

Compliance

[Wayne VanOsdol, VP Compliance](#) (1714)
[Jo Anne McNabb, Compliance Admin](#) (1730)

Mitigation, Reliability Standards, Training & Education

[Jim Burley, Sr. Director, Mitigation, Reliability Standards, Training and Education](#) (1748)
[Jennifer Matz, Mit & Stnd Administrator](#) (1740)

Standards

[Carol Gerou, Standards Manager](#) (1735)

Operations

[Dan Schoenecker, VP Operations](#) (1753)
[Kristine Hutchens, Operations Admin](#) (1749)

Assessments

[Salva Andiappan, Mgr Reliability Assessments and Performance Analysis](#) (1719)

Event Analysis and Situational Awareness

[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

Our Mission

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

EMPLOYEE NEWS

Congratulations to **Jacob Phillips**, MRO Enforcement Attorney, for passing the MN bar exam administered in February 2011. The swearing in ceremony will take place on May 6. Jake was admitted to practice law in North Dakota in 2009.

MRO is pleased to welcome **Kenneth Gartner** and **Joseph Gay**, who joined MRO in April as Compliance CIP Audit Specialists.

For open positions within MRO, please visit the [career page](#).

ABOUT MRO

MRO is a non-profit organization dedicated to ensuring the reliability and security of the Bulk Power System (BPS) and operates under delegated authority from regulators in both the U.S. and Canada. MRO works to develop and ensure compli-

ance 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**

MRO Calendar of Events

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

Date	Time	Group	Location
May 2011			
May 16	12:00 - 5:00	Protective Relay Subcommittee Meeting	Crowne Plaza MSP Bloomington, MN
May 17	8:00 - 12:00		
May 17	8:00 - 3:00	Operating Committee	Crowne Plaza MSP Bloomington, MN
May 17	9:00-12:00	Compliance Committee	TBD
May 18	8:30 - 3:30	Planning Committee Meeting	Crowne Plaza MSP Bloomington, MN
May 19	8:00 - 5:00	Standards Committee Meeting	Crowne Plaza MSP Bloomington, MN
June 2011			
June 3	8:00 - 3:00	Compliance Committee Meeting	Conference Call/WebEx
June 16	TBD	Board of Directors	TBD
June 21	8:00 - 5:00	Spring Reliability Conference	Embassy Suites Airport Bloomington, MN
June 22	8:00 - 12:00		
June 22	8:00 - 4:00	Model Building Subcommittee Meeting	Crowne Plaza MSP Bloomington, MN

MIDWEST RELIABILITY ORGANIZATION

2774 Cleveland Ave N. Roseville, MN 55113 Ph: 651-855-1760 Fx: 651-855-1712
www.midwestreliability.org